(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101124765 B
(45)授权公告日 2013.08.07

(21)申请号 200480034296.3
(22)申请日 2004.11.19
(30)优先权数据
60/523,398 2003.11.19 US
(85)PCT申请进入国家阶段日
2006.05.19
(86)PCT申请的申请数据
PCT/US2004/039126 2004.11.19
(87)PCT申请的公布数据
WO2005/052752 EN 2005.06.09
(73)专利权人 科尔街有限公司
地址 美国马萨诸塞州
(72)发明人 戴维·恩贝里
(74)专利代理机构 北京金信立方知识产权代理有限公司 11225
代理人 朱梅
(51)Int.Cl.
H04L 9/00(2006.01)
G06F 17/30(2006.01)

(56)对比文件
US 6097811 A,2000.08.01, 全文.
US 6134550 A,2000.10.17, 全文.
US 2002/0046340 A1,2002.04.18, 说明书[0014]-[0117]节, 附图2-12.
US 2003/0130947 A1,2003.07.10, 说明书[0012]-[0103]节、附图2-8.

审查员 李凯

权利要求书2页 说明书9页 附图6页

(54)发明名称

分布式代表路径发现与确认

(57)摘要

为系统提供路径确认信息包括确定系统证书子集和至少一信任根之间的路径，在请求路径确认信息之前将每一路径均保存在表中，及响应于请求路径确认信息的请求取回保存在表中的确认信息。提供路径确认信息还包括数字签署确认信息。提供路径确认信息还包括对确认信息应用约束条件并仅提供满足约束条件的确认信息。确定路径包括建立可信根及证书子集的有向图并对图执行深度优先的非循环搜索。

CN 101124765 B

1. 为系统提供路径确认信息的方法，包括：

确定系统的多个证书中的每一个和至少一信任根之间的路径；

在请求从目标证书到所述至少一信任根的信任路径的路径确认信息之前将所有路径的确认信息保存在表中；及

响应于所述请求从保存在表中的所有路径的确认信息中取回所述信任路径的确认信息并且将保存在表中并从表中取回的所述信任路径的确认信息提供给依赖方而不要求任何额外的处理时间即可检索用于所述信任路径的实时确认的证书状态信息。

2. 根据权利要求 1 的方法，还包括：

数字签署确认信息。

3. 根据权利要求 1 的方法，还包括：

对确认信息应用约束条件并仅提供满足约束条件的确认信息。

4. 根据权利要求 1 的方法，其中确定路径包括建立可信根及所述多个证书的有向图并对图执行深度优先的非循环搜索。

5. 根据权利要求 1 的方法，其中表使用可信的根进行索引。

6. 根据权利要求 1 的方法，其中表使用证书进行索引。

7. 根据权利要求 1 的方法，还包括：

接收所述多个证书的废除状态的证明；

在请求路径确认信息之前保存证明；及

响应于请求路径确认信息的请求取回证明及确认信息。

8. 根据权利要求 7 的方法，还包括：

数字签署确认信息及证明。

9. 根据权利要求 7 的方法，还包括：

对确认信息应用约束条件且仅提供满足约束条件的确认信息。

10. 根据权利要求 7 的方法，其中确定路径包括建立可信根及所述多个证书的有向图并对图执行深度优先的非循环搜索。

11. 根据权利要求 7 的方法，其中证明被保存在包含确认信息的表中。

12. 根据权利要求 11 的方法，其中表使用可信的根进行索引。

13. 根据权利要求 11 的方法，其中表使用证书进行索引。

14. 根据权利要求 7 的方法，其中证明被保存在与包含确认信息的表分开的其它表中。

15. 根据权利要求 14 的方法，其中其它表使用可信的根进行索引。

16. 根据权利要求 14 的方法，其中其它表使用证书进行索引。

17. 根据权利要求 1 的方法，其中所述多个证书包括可信的根、向终端用户发出证书的管理机构、及担保其它管理机构的管理机构。

18. 根据权利要求 17 的方法，其中所述多个证书还包括终端用户证书。

19. 为系统提供路径确认信息的服务器，包括：

确定系统的多个证书中的每一个和至少一信任根之间的路径的模块；

在请求从目标证书到所述至少一信任根的信任路径的路径确认信息之前将所有路径的确认信息保存在表中的模块；及

响应于所述请求从保存在表中的所有路径的确认信息中取回所述信任路径的确认信

息并且将保存在表中并从表中取回的所述信任路径的确认信息提供给依赖方而不要求任何额外的处理时间即可检索用于所述信任路径的实时确认的证书状态信息的模块。

20. 根据权利要求 19 的服务器，还包括：

数字签署确认信息的模块。

21. 根据权利要求 19 的服务器，还包括：

对确认信息应用约束条件并仅提供满足约束条件的确认信息的模块。

22. 根据权利要求 19 的服务器，其中确定路径的模块建立可信根及所述多个证书的有向图并对图执行深度优先的非循环搜索。

23. 根据权利要求 19 的服务器，其中表使用可信的根进行索引。

24. 根据权利要求 19 的服务器，其中表使用证书进行索引。

25. 根据权利要求 19 的服务器，还包括：

接收所述多个证书的废除状态证明的模块；

在请求路径确认信息之前保存证明的模块；及

响应于请求路径确认信息取回证明及确认信息的模块。

26. 根据权利要求 25 的服务器，还包括：

数字签署确认信息及证明的模块。

27. 根据权利要求 25 的服务器，还包括：

对确认信息应用约束条件且仅提供满足约束条件的确认信息的模块。

28. 根据权利要求 25 的服务器，其中确定路径的模块建立可信根及所述多个证书的有向图并对图执行深度优先的非循环搜索。

29. 根据权利要求 25 的服务器，其中证明被保存在包含确认信息的表中。

30. 根据权利要求 29 的服务器，其中表使用可信的根进行索引。

31. 根据权利要求 29 的服务器，其中表使用证书进行索引。

32. 根据权利要求 25 的服务器，其中证明被保存在与包含确认信息的表分开的其它表中。

33. 根据权利要求 32 的服务器，其中其它表使用可信的根进行索引。

34. 根据权利要求 32 的服务器，其中其它表使用证书进行索引。

35. 根据权利要求 19 的服务器，其中所述多个证书包括可信的根、向终端用户发出证书的管理机构、及担保其它管理机构的管理机构。

36. 根据权利要求 35 的服务器，其中所述多个证书还包括终端用户证书。

分布式代表路径发现与确认

[0001] 相关申请交叉索引

[0002] 本申请要求 2003 年 11 月 19 日申请的美国临时申请 60/523,398 的优先权，其通过引用组合于此。

[0003] 发明背景

1. 技术领域

[0004] 本申请涉及数据安全和确认领域，特别是涉及验证和确认数字证书及其它信息的领域。

2. 背景技术

[0005] 能够确定数字证书的状态是有用的，其包括确定证书是否被正当地发出和 / 或证书在其过期之前是否已被废除。现在有很多确定单个数字证书的状态的技术。例如，美国专利 5,666,416 和 5,717,758 描述了提供单个证书状态的技术。其它散布和确定证书状态的技术也广为人知，包括证书废除表 (CRL)，其为数字签署的作废证书的列表。

[0006] 验证数字证书要求必须信任数字证书的发行人和 / 或作废信息的签署人，二者可以是也可以不是同一实体。在数字证书的情况下，“信任”发行人和 / 或作废信息的签署人涉及这样一个事实，即发行人和 / 或签署人是具有对应于秘密密钥的有效公钥的已知管理机构，所述密钥用于签署证书和 / 或作废信息。例如，用户可接收由管理机构 A 数字签署的数字证书，也可接收由不同的管理机构 A’ 签署的最新 CRL（其不包含数字证书）。然而，用户可能想要能够同时信任 A 及 A’ 连同它们的公钥（对应于用于签署证书和 CRL 的秘密密钥）以能够认同证书。

[0007] 有多种机制用于帮助发布证书及作废信息的另外的未知管理机构的散布与信任。在一些情况下，可能使可信管理机构数字签署信息（或确认信息）以验证另外的未知管理机构。其后，先前未知的管理机构可呈现数字签署的信息（如数字证书和 / 或作废信息），其可使用先前未知的管理机构的公钥进行验证。例如，如果用户不知道或不信任管理机构 A1 和 A2 的数字签名，但用户知道和信任管理机构 A3，则用户可获得（或被呈现以）由 A3（因而由 A3 担保）数字签署的、表明 A1 和 A2 是可信赖管理机构的信息。因此，如果该用户被呈现以 A1 签署的数字证书及 A2 签署的 CRL（其未列出数字证书），用户可使用由 A3 担保的信息验证所呈现的证书的有效性。

[0008] 另外还有可用在管理机构担保其它管理机构情况中的嵌套机制。例如，通过引用组合于此的美国专利 5,717,759 公开了这样的技术：第一管理机构 A1 担保第二管理机构 A2、第二管理机构 A2 担保第三管理机构 A3 等，直到嵌套达到潜在用户信任的管理机构为止。在一些情况下，担保可包括提供担保机构的数字签名。

[0009] 尽管嵌套和其它机制是有用的，但在某些情况下，用户可能被呈现以数字证书和 / 或作废信息和 / 或某些其它信息，但没有简单直接的机制可确定证书 / 作废信息的签署人可被信任，因而用户不能确定数字证书在当前是否有效。因此，解决该问题是有用的。

发明内容

[0010] 根据本发明，为系统提供路径确认信息包括确定系统证书子集和至少一信任根之间的路径，在请求路径确认信息之前将每一路径均保存在表中，及响应于请求路径确认信息的请求取回保存在表中的确认信息。提供路径确认信息还包括数字签署确认信息。提供路径确认信息还包括对确认信息应用约束条件并仅提供满足约束条件的确认信息。确定路径包括建立可信根及证书子集的有向图并对图执行深度优先的非循环搜索。表可使用可信的根或使用证书进行索引。提供路径确认信息还包括接收证书子集的废除状态的证明，在请求路径确认信息之前保存证明，及响应于请求路径确认信息的请求取回证明及确认信息。提供路径确认信息还包括数字签署确认信息及证明。提供路径确认信息还包括对确认信息应用约束条件且仅提供满足约束条件的确认信息。确定路径包括建立可信根及证书子集的有向图并对图执行深度优先的非循环搜索。证明可被保存在包含确认信息的表中。表可使用可信的根进行索引。表可使用证书进行索引。证明可被保存在与包含确认信息的表分开的其它表中。其它表可使用可信的根或使用证书进行索引。证书子集可包括可信的根、向终端用户发出证书的管理机构、及担保其它管理机构的管理机构。证书子集还可包括终端用户证书。

[0011] 根据本发明，为系统提供路径确认信息的计算机程序产品包括包含计算机程序产品的可执行代码的存储介质，确定系统证书子集和至少一信任根之间的路径的可执行代码，在请求路径确认信息之前将每一路径保存在表中的可执行代码，及响应于请求路径确认信息的请求取回保存在表中的确认信息的可执行代码。计算机程序产品还包括数字签署确认信息的可执行代码。计算机程序产品还包括对确认信息应用约束条件并仅提供满足约束条件的确认信息的可执行代码。确定路径的可执行代码建立可信根及证书子集的有向图并对图执行深度优先的非循环搜索。表可使用可信的根进行索引。表可使用证书进行索引。计算机程序产品还包括接收证书子集的废除状态的证明的可执行代码，在请求路径确认信息之前保存证明的可执行代码，及响应于请求路径确认信息的请求取回证明及确认信息的可执行代码。计算机程序产品还包括数字签署确认信息及证明的可执行代码。计算机程序产品还包括对确认信息应用约束条件且仅提供满足约束条件的确认信息的可执行代码。确定路径的可执行代码建立可信根及证书子集的有向图并对图执行深度优先的非循环搜索。证明可被保存在包含确认信息的表中。表可使用可信的根或使用证书进行索引。证明可被保存在与包含确认信息的表分开的其它表中。其它表可使用可信的根或使用证书进行索引。证书子集可包括可信的根、向终端用户发出证书的管理机构、及担保其它管理机构的管理机构。证书子集还可包括终端用户证书。

[0012] 根据本发明，服务器包括处理器、连到处理器的内存储器、提供在内存储器上的确定证书子集和至少一可信根之间的路径的可执行代码、提供在内存储器上的在请求路径确认信息之前将每一路径保存在表中的可执行代码、及提供在内存储器上的响应于请求路径确认信息的请求取回保存在表中的确认信息的可执行代码。服务器可包括提供在内存储器上的数字签署确认信息的可执行代码。服务器可包括提供在内存储器上的、对确认信息应用约束条件并仅提供满足约束条件的确认信息的可执行代码。确定路径的可执行代码建立可信根及证书子集的有向图并对图执行深度优先的非循环搜索。表可使用可信的根或使用

证书进行索引。服务器可包括提供在内存储器上的接收证书子集的废除状态的证明的可执行代码，提供在内存储器上的在请求路径确认信息之前保存证明的可执行代码，及提供在内存储器上的响应于请求路径确认信息的请求取回证明及确认信息的可执行代码。服务器还包括提供在内存储器上的数字签署确认信息及证明的可执行代码。服务器可包括提供在内存储器上的对确认信息应用约束条件且仅提供满足约束条件的确认信息的可执行代码。确定路径的可执行代码建立可信根及证书子集的有向图并对图执行深度优先的非循环搜索。证明可被保存在包含确认信息的表中。表可使用可信的根或使用证书进行索引。证明可被保存在与包含确认信息的表分开的其它表中。其它表可使用可信的根或使用证书进行索引。证书子集可包括可信的根、向终端用户发出证书的管理机构、及担保其它管理机构的管理机构。证书子集还可包括终端用户证书。

附图说明

[0013] 图 1 为根据在此描述的系统的实施例的非置信的代表路径 / 确认服务器。

[0014] 图 2 为根据在此描述的系统的实施例的可信代表路径 / 确认服务器。

[0015] 图 3 为根据在此描述的系统的实施例的两个互连的区域，每一区域包含本地证书信息。

[0016] 图 4 为根据在此描述的系统的实施例使用网络将证书信息传送给用户的情形。

[0017] 图 5 为根据在此描述的系统的实施例预计算信任路径的流程图。

[0018] 图 6 为根据在此描述的系统，与填充证书及信任路径的表有关的通过信任路径迭代的流程图。

[0019] 图 7A、7B 和 7C 为根据在此描述的系统的实施例的包含信任路径和 / 或证明的表。

[0020] 图 8 为根据在此描述的系统的实施例，返回预先计算的信任路径和 / 或证明的流程图。

[0021] 图 9 为根据在此描述的系统的实施例，由可信的代表路径 / 确认服务器执行的处理的流程图。

具体实施方式

[0022] 提供单个证书状态信息的技术公知为用于验证证书和 / 或数字签署证书的管理机构的技术。例如，参见美国专利 5,420,927、5,604,804、5,610,982、6,097,811、6,301,659、5,793,868、5,717,758、5,717,757、6,487,658 及 5,717,759 的公开内容，这些专利均通过引用组合于此。在此描述的系统可使用这些专利中的一个或多个公开的技术，可能与一个或多个其它适当的技术结合。可被使用的技术包括，单独地或任何形式的组合，完整 CRL、分割的 CRL、CRL 增量、OCSP 响应（单独地或成组）、迷你型 CRL（逐位压缩的 CRL）、VToken（单向散列链）、及各种 Merkle 树或其它树形。

[0023] 路径发现涉及发现任意证书和用户的信任根之一之间的信任路径（信任关系）的过程，其为对应于用户信任的管理机构的数字证书。信任路径是从一证书到另一证书的授权链，其在一端具有目标证书而在另一端具有信任根。例如，如果证书 C1 对应于可信的管理机构 A1，及 A1 签署未知管理机构 A2 的 C2，管理机构 A2 签署未知管理机构 A3 的 C3，未知管理机构 A3 签署目标证书，则从 C1（信任根）到目标证书的信任路径为 C1 到 C2、C2 到

C3、及 C3 到目标证书。

[0024] 在一些情况下，无论信任路径中的所有证书在何时在本地可用，路径发现可由用户以相当简单直接的方式在本地执行。然而，在一些情况下，包括那些具有基于交叉认证的联合信任模型的情况，用户可能不具有执行本地路径发现所需要的所有信息。

[0025] 同样还应注意，即使完整的信任路径已在信任根和目标证书之间发现时，仍然要考虑信任路径上的一个或多个证书自其发布后可能已被废除。路径确认指证实信任路径中所有证书的当前状态，包括证书的有效性（作废状态）并考虑对应于证书的使用的任何及所有规则和/或约束条件（如检查安全策略）。集合信任路径中每一证书的废除状态信息在某些情况下对某些用户而言可能相当困难（如那些阻止访问公用网的特殊防火墙设置）。因此，能够提供可在单一事务中验证证书的服务是有用的。这可以这样实现：首先确定信任路径，接收关于信任路径中的证书的废除信息（和/或约束信息），及处理所接收的信息以验证目标证书。

[0026] 参考图 1，非置信代表路径发现/确认 (UDPDV) 服务器 30 接收确定一个或多个信任根的信息（可信管理机构的证书）及对应于用户希望确认的目标证书（或其它信息/数据）的标识符作为输入。可选地，除了接收信任根作为输入以外或代替接收信任根作为输入，UDPDV 服务器 30 可被预先配置以信任根。

[0027] 当然，如果用户已经信任发出目标证书的管理机构且用户有权使用目标证书（可能及可信管理机构的证书）的可靠废除信息，则用户可使用该信息验证目标证书而不必使用 UDPDV 服务器 30。因而，UDPDV 服务器 30 在这样的情况是有用的：用户想验证目标证书的状态，但用户不信任（知道）发出目标证书的管理机构和/或用户未拥有关于目标证书（可能及发出目标证书的管理机构的证书）的可靠废除信息。

[0028] UDPDV 服务器 30 处理对其的输入以确定目标证书和信任根（或输入或预先配置在 UDPDV 服务器 30 中，如上所述）之间的一个或多个信任路径。应注意，在许多情况下，证实信任路径中没有证书已被废除同样有用（例如，指示管理机构的秘密密钥的泄密情况）。在这样的情况下，使 UDPDV 服务器 30 也提供已确认废除信息（如 CRL 或 OCSP 响应）形式的证明是有用的。因而，在一些实施例中，UDPDV 服务器 30 还可为信任路径中的证书提供证明。

[0029] 因此，在图 1 中公开的实施例中，UDPDV 服务器 30 集合目标证书的信任路径信息，及可选地，还集合路径元素的废除信息。UDPDV 服务器 30 向用户的输出不被单独鉴别（如签署）。相反，UDPDV 服务器 30 将信任路径的所有单个元素（及，可选地，证明）返回给用户，其继而单独验证信任路径的正确性及信任路径元素（证书）的有效性。UDPDV 服务器 30 的运行将在本文别处详细描述。

[0030] 参考图 2，可信代表路径发现/确认服务器 40 接收用户的信任根及对应于用户希望验证的目标证书（或其它信息/数据）的标识符作为输入。可选地，除了接收信任根作为输入以外或代替接收信任根作为输入，可信的代表路径发现/确认服务器 40 可被预先配置以信任根。

[0031] 可信的代表路径发现/确认服务器 40 输出表明目标证书（或其它信息/数据）是否有效的结果。在于此描述的实施例中，服务器 40 对提供给用户的信息执行其自身的密码鉴别。在该实施例中，服务器 40 可签署因此提供的响应，其允许服务器 40 提供少量数据

给用户（如“是，你可信任证书 X”）。然而，这样的实施设定用户明确信任可信的代表路径服务器 40 的内部运行的完整性和正确性。如果服务器 40 被泄密，则服务器 40 可被不适当地用于鉴别确认任何证书的响应，不管来源或当前状态如何。

[0032] 服务器 30、40 可由计算机工作站提供，其具有处理器和用于保存可执行代码和数据的内存储器、提供在通用计算机中的一个或多个软件模块、专用硬件、或能够提供在此描述的功能的硬件和软件的任意组合。对于在此描述的系统，UDPDV 服务器 30 可由一个或多个轻便服务器提供，其不需要具备鉴别能力（如用于数字签名的私钥）。

[0033] UDPDV 服务器 30 可被定期配置以两种类型的信息列表。第一类型的列表包含一组可用在路径确认中的证书，且其在于此的实施例中代表所有或几乎所有可为 UDPDV 服务器 30 接近（如通过网络）的证书。在另一实施例中，第一类型的列表包含仅用于发布证书和废除信息的管理机构及担保这些管理机构的管理机构的证书，而不必包含所有或甚至任何终端用户证书。第一类型的列表可包含自签署的根证书（可信的根），其用作信任锚。可信的根可由系统用户信任的管理机构签署。第一类型的列表还可包含发行人 (aka“认证授权”) 证书，其用于发布证书的管理机构、发布废除信息的管理机构、担保其它管理机构的管理机构。在一实施例中，第一类型的列表还可包含终端用户证书，而在另一实施例中，第一类型的列表不包含终端用户证书。如在此所述的，证书的第一类型列表可用于提供路径发现服务。

[0034] 在 UDPDV 服务器 30 中提供的第二类型的列表可包括预先产生的证书状态证明。每一证明可包含一个或多个证书（来自第一列表）在固定时间间隔期间的状态，且证明可被安全鉴别，如使用数字签名。如本文别处所描述的，证明可用于提供路径确认服务。证明可由任何适当的手段提供，包括 CRL、OCSP 响应、VToken 等。

[0035] 检查可信的根和目标证书之间的路径在本领域是公知的并在证书标准（如 RFC3280）中有明确记载。然而，通过大量证书发现信任路径基于库中的证书量可能需要指数时间。这在某些情形下和 / 或对于小量证书是可接受的，但在其它情形下不可接受，如大的同盟管理机构团体的情况。

[0036] 在此描述的系统设计来在发现请求时以对数时间或恒定时间执行路径发现，其首先预计算每一可信的根证书和所有其它可由发布证书和 / 或担保其它管理机构的管理机构获得的证书之间的信任路径。当 UDPDV 服务器 30 接收新的证书列表时（或被连接到新的证书源时），服务器可通过 N 矩阵预计算 M，其中 M 是可信的根的数量，N 是证书总数。矩阵中的每一单元（如行 r1 和列 c1）可包含一个或多个从由行 r1 表示的特定可信根到由列 c1 表示的特定证书的合法路径，否则包含空集以表明不可能有路径。可选地，每一单元（或相似表的每一单元）还可包含适当的证明以提供确认。

[0037] 当验证目标证书的用户请求到达时，UDPDV 服务器 30 使用预计算的矩阵查寻该用户的可信根并查寻发出目标证书的管理机构，可选地，及查寻发布目标证书的废除信息的管理机构（如果不同于发证管理机构）以发现其间的一个或多个有效路径。这可以恒定时间查寻完成，因为路径已被预先计算并保存在 UDPDV 服务器 30 中。应注意，如果有一个以上的可能信任路径或如果有与信任路径相关的约束条件（如名称或政策约束条件），所述约束条件以任何方式限制信任路径中任何证书的使用，则需要应用与发现的任何信任路径相对的路径策略。通过预先计算所有可能的路径，UDPDV 服务器 30 可以相当高的性能可扩

缩性为大的团体提供路径发现。

[0038] 除路径发现以外，UDPDV 服务器 30 还可为信任路径的元素（证书）提供确认信息（证明）。在一实施例中，UDPDV 服务器 30 为信任路径中的每一元素（证明）实时获得证明（如 CRL 或 OCSP 响应形式的证明），其接着被提供给用户。尽管可能通过缓存证明而改善性能，但当证明被实时获得时，仍然有可能在请求时不是最佳性能。在另一实施例中，在 UDPDV 服务器 30 中有路径确认机制，其定期接收 UDPDV 服务器 30 使用的每一证书与产生信任路径有关的预先产生的、纹理细密的状态证明。对于该实施例，UDPDV 服务器 30 能够快速访问所有需要的确认信息，其可在不要求任何额外的处理时间的情况下提供给依赖方，从而检索用于实时确认的证书状态信息。

[0039] 还应注意，如果证明被进栈到 UDPDV 服务器 30（如以预签署的 OCSP 响应的形式），UDPDV 服务器 30 对信任路径中的每一证书的状态可进行瞬时本地访问。对于某些实施例，UDPDV 服务器 30 在返回路径代表团的信任路径之前证实信任路径的状态。UDPDV 服务器 30 还可将状态证明返回给用户以允许由用户进行信任路径的本地完全确认。证明的各不相同、预先产生的特性（如预先产生的 OCSP 响应）允许有效使用网络资源，同时避免任何与可信的在线服务器相关联的安全风险。

[0040] 参考图 3，图 50 示出了第一区 52 和分开的第二区 54。区 52、54 可通过任何适当的手段（如网络或直接连接）互连以能在其间交换信号。第一区 52 包括多个证书 62-64。第二区 54 包括多个不同的证书 66-68。第一区 52 表示可由那里的用户本地管理和访问的局部性。类似地，第二区 54 表示可由那里的不同用户本地管理和访问的另外的局部性。因此，例如，在区 52 中的用户可本地访问证书 62-64 中的任意一个或全部。

[0041] 在区 52，证书 62 是管理机构 A1 的自证实根证书（可信的根）。证书 62 还通过使 A1 签署证书 63 而证实管理机构 A2 的证书 63。证书 63 证实管理机构 A3 的证书 64。应注意，在该例子中，如果用户信任 A1，则用户也应信任 A2（由 A1 担保）且还应信任 A3（由 A2 担保）。在区 54，证书 66 是管理机构 A1’的自证实根证书（可信的根）。证书 66 还证实管理机构 A2’的证书 67 及证书 67 证实管理机构 A3’的证书 68。证书 62 与证书 66 交叉证明，使得证书 62、66 中的每一个证实证书 62、66 中的另一个。

[0042] 如果在区 52 的用户被呈现以由 A3’签署的目标证书，如果在区 52 的用户开始仅知道（及信任）A1、A2 和 A3，则用户不能立即验证目标证书是否有效。然而，应注意，管理机构 A2’担保管理机构 A3’，及管理机构 A1’担保管理机构 A2’。还应注意管理机构 A1 担保管理机构 A1’。因此，假设在区 52 的本地用户信任 A1，则对于该用户有下述信任路径：从证书 62 到证书 66 到证书 67 到证书 68 到已被 A3’签署的目标证书。因而，用户可接受由管理机构 A3’签署的目标证书，因为有从目标证书到已由可信的管理机构 A1 签署的证书 62 的信任路径。同样，如本文别处所述，可能为沿信任路径的每一证书及发布废除信息的管理机构（如果不同于发证机构）提供确认信息（有效性证明），使得接收信任路径的用户也可接收证书 62、66-68 的最新废除信息。

[0043] 参考图 4，图 80 示出了用户从通过网络 88 连到用户 82 的多个数据存储设备 84-86 中的一个或多个接收证书信息（包括信任路径信息及可能的确认信息）。在于此的实施例中，网络可以是因特网，尽管也可使用其它适当的网络，包括在用户和一个或多个数据存储设备 84-86 之间提供直接连接的网络。还应注意，用户 82 可本地保存部分证书信息。在于

此的实施例中，用户 82 可被呈现以一个或多个用户希望确定其有效性的证书。在某些情况下，用户 82 可使用本地数据确定证书的有效性。然而，如本说明书别处所描述的，在其它情形下，用户 82 从类似数据存储设备 84-86 的其它源获得证书信息是必要的。在这些情况下，证书信息及其请求可在网络 88 上以简单直接的方式在用户和存储设备之间传输。当然，任何适当的连通和信息请求 / 传输技术均可用于提供在此描述的功能。

[0044] 参考图 5，流程图 100 示出了初始化 UDPDV 服务器 30 以包含可信的根（可信管理机构的根证书）及发出证书和 / 或担保其它管理机构的一个或多个其它证书之间的所有路径。如本说明书别处所述的，每一信任路径可被预先计算，从而当用户呈现目标证书时，UDPDV 服务器可查阅表、查寻发出目标证书的管理机构（或查寻目标证书本身），并提供预先计算的从目标证书到可信的根证书的信任路径。同样，如在此所述的，UDPDV 服务器 30 也可为信任路径中的证书提供表明证书尚未被废除的证明。

[0045] 流程图 100 的处理在第一步骤 102 开始，为所有其信息将被保存的证书建立有向图。有向图是本领域公知的数学作图。对于在此的实施例，系统中的所有证书包括终端用户证书均被使用。对于另一实施例，终端用户证书不被包括，或者仅包括部分终端用户证书。在步骤 102，所建立的有向图表示证书之间的关系，其中图的边缘（连接线）指示第一管理机构（对应于连接在边缘一端的证书）已担保第二管理机构（对应于连接在边缘另一端的证书）。

[0046] 在步骤 102 之后是步骤 104，下标变量被设定为等于 1。下标变量 I 被用于通过 UDPDV 服务器 30 的每一可信的根证书进行迭代。如本说明书别处所述，可信的根证书被提供为 UDPDV 服务器 30 的输入或被预先配置在 UDPDV 服务器 30 中。

[0047] 在步骤 104 之后是测试步骤 106，确定下标变量 I 是否大于可信的根证书的数量。如果是，则处理结束。否则，控制从测试步骤 106 转到步骤 108 以确定从可信的根证书（对应于下标变量 I）到有向图中的所有其它证书的所有路径。步骤 108 将在本说明书别处详细讨论。在步骤 108 之后是步骤 112，递增下标变量 I。在步骤 112 之后，控制转回到如上所述的测试步骤 106。

[0048] 参考图 6，流程图 120 更详细地示出了连同图 5 的流程图 100 的步骤执行的处理。对于每一可信的根，对有向图执行深度优先的非循环搜索以发现所有信任路径。对于在每一路径中发现的每一证书，在表中进行登记，其指示从证书到可信根的可信路径。

[0049] 处理在第一步骤 122 开始，确定是否有更多的路径要被检查。应注意，在某些情况下，可能存在无路径到其的可信根。然而，在大多数情况下，预计每一可信的根将具有至少一到其的路径。如果在测试步骤 122 确定没有更多的路径需要被检查（处理），则处理结束。否则，控制从测试步骤 122 转到步骤 124，其中下一路径使用对有向图的深度优先的非循环搜索进行确定。在步骤 124 之后是步骤 126，证书指针 CP 被设定为指向被检查（处理）的路径的末端。

[0050] 在步骤 126 之后是测试步骤 128，确定 CP 是否指向可信的根，因而表明所有路径均已被遍历。如果是，则控制从测试步骤 128 转回到如上所述的步骤 122 以开始下一迭代。否则，控制从测试步骤 128 转到步骤 132，从 CP 到可信的根的路径被记录在保存证书及至其的可信路径的表中（如本说明书别处所述）。在一实施例中，在表的由 CP 指向的证书索引的部分，从 CP 到可信的根的路径在步骤 132 进行记录。在步骤 132 之后是步骤 134，CP 被

设定为指向路径中在前的证书。因而，CP 初始指向路径的末端，随后指向路径中在前的证书，即朝向可信的根往回工作。在步骤 134 之后，控制转回到如上所述的测试步骤 128。

[0051] 参考图 7A，表 140 包括由系统中的证书索引的第一部分 142，并具有到每一证书的可信路径作为其元素。表 140 还可包括同样由系统中的证书索引的第二部分 144。第二部分具有描述证明（如 OCSP 响应、CRL 等）的元素，所述证明指示每一相应证书的废除状态。在于此描述的实施例中，在第二部分 144 中提供的证明对应于索引证书，从而由 C2 索引的表项目对应于 C2 的证明。在另一实施例中，在第二部分 144 中提供的证明对应于对于第一部分 142 中特定项的所有路径中的所有证书。因此，例如，在第二部分 144 中提供的证明连同证书 C2 对应于在第一部分 142 用于 C2 的项中提供的信任路径中的所有证书。

[0052] 在一些实施例中，可能排除部分 142、144 之一。因此，例如，在只有部分 142 的实施例中，UDPDV 服务器 30 提供预先计算的信任路径，但不提供证明。对于这样的实施例，用户或完全放弃证明或实时获得证明或其结合（即为路径中的部分证书获取证明而不获取其它证书的证明）。对于只有部分 144 的实施例，信任路径可被实时确定，且来自部分 144 的预先计算的证明可由 UDPDV 服务器 30 提供。

[0053] 参考图 7B，另一实施例使用根据证书索引的单表 140’，信任路径和证明均被提供为表 140’的元素。

[0054] 参考图 7C，另一实施例示出了表的另一结构 140″。表 140″可根据特定的可信根证书 TR1、TR2、…、TRN 及其它证书 C1、C2、…、CN 进行索引。在表 140″的项的元素包含信任路径及（可选地）证明“P/P”，从而用于可信的根 TRx 及证书 Cy 的项包含一个或多个从 Cy 到 TRx 的信任路径（如果存在），及可选地，包含一个或多个仅用于 Cy 的证明（一实施例）或用于信任路径中的所有证书的证明（另一实施例）。

[0055] 参考图 8，流程图 150 示出了 UDPDV 服务器 30 服务于来自用户的请求信任路径及其中证书的证明时的处理步骤。如本说明书别处所述，UDPDV 服务器 30 可被呈现以特定的目标证书，UDPDV 服务器 30 为其提供信任路径及指明信任路径中每一证书的状态的证明。在一实施例中，信任路径被提供给发出目标证书的管理机构的证书，及可选地，提供给发布目标证书的废除信息的管理机构（如果不同于发证机构）的证书。在另一实施例中，UDPDV 服务器 30 提供信任路径及目标证书自身的废除信息。

[0056] 处理在第一步骤 152 开始，确定对目标证书或其发行人是否有任何信任路径可用。如果否，则控制从步骤 152 转到步骤 154，在该步骤执行特殊的处理。在步骤 154 执行的特殊处理可包括公布出错消息和 / 或以某些其它方式向用户指明没有为目标证书发现信任路径。在步骤 154 之后，处理结束。

[0057] 如果在测试步骤 152 确定有信任路径可用，则控制从测试步骤 152 转到步骤 156，下一信任路径被选择以进行处理。在于此的实施例中，系统可通过每一信任路径（由表 140、表 140’、或表 140″提供）进行迭代以发现目标证书（或其发行人）和一个或多个可信的根证书之间的适当信任路径。在步骤 156 选择的下一信任路径可使用大量标准中的任意一个进行选择，如最短的路径、包含特定证书的路径等。

[0058] 在步骤 156 之后是测试步骤 158，确定对在步骤 156 选择的特定信任路径（信任路径的证书）是否有约束条件。如本说明书别处所述，可能有一个或多个约束条件阻止特定信任路径的使用，如因为某些目的一个或多个证书不被接受。如果在测试步骤 158 确定

有约束条件使信任路径被检查为不可接受，则控制从测试步骤 158 转回到如上所述的步骤 152。否则，控制从测试步骤 158 转到步骤 162，确定用于信任路径中的证书的证明是否已被请求。如果否，则控制从步骤 162 转到步骤 164，目标证书（或其发行人）及可信的根证书之间的信任路径被返回给用户。在步骤 164 之后，处理结束。

[0059] 如果在测试步骤 162 确定证明已被请求，则控制从测试步骤 162 转到步骤 166，（来自表 140、表 140'、或表 140″）的证明被获得。在其它实施例中，证明可被实时获取。在步骤 166 之后是步骤 168，返回信任路径和证明。在步骤 168 之后，处理结束。

[0060] 如本说明书别处所述，在某些情形下，用户可能希望使用可信的分布式代表路径发现和确认服务器 40，其返回指明特定证书是否有效的经签署（或经鉴别）的消息。服务器 40 可签署指明特定证书是否可接受的消息。用户依赖于来自服务器 40 的经签署的响应，而不必直接知道或检查路径和 / 或确认信息。

[0061] 参考图 9，流程图 180 示出了服务器 40 在建立和返回指明特定目标证书是否有效的签署消息时所执行的步骤。处理在第一步骤 182 开始，可信的路径和证明根据本说明书别处所述的那样获取。在步骤 182 之后是测试步骤 184，其中信任路径和证明被检查以确定目标证书是否有效。在步骤 184 的确定可使用在步骤 182 获得的信任路径和证明进行。如果在测试步骤 184 确定目标证书有效，则控制从测试步骤 184 转到步骤 186，表明目标证书有效的、肯定的消息被产生。否则，如果在测试步骤 184 确定目标证书无效，则控制从测试步骤 184 转到步骤 188，产生否定消息。

[0062] 在步骤 186 或步骤 188 之后是步骤 192，消息由服务器 40 数字签署。在步骤 192 之后是步骤 194，经签署的结果被返回给用户。在步骤 194 之后，处理结束。

[0063] 在此描述的系统可使用通用计算机上的硬件和 / 或软件的任意适当组合实施，所述软件包括在专用硬件上的存储器中提供的软件。

[0064] 在本发明已结合多个实施例公开的同时，其修改对本领域技术人员而言是容易的。因此，本发明的实质和范围在下述权利要求中提出。

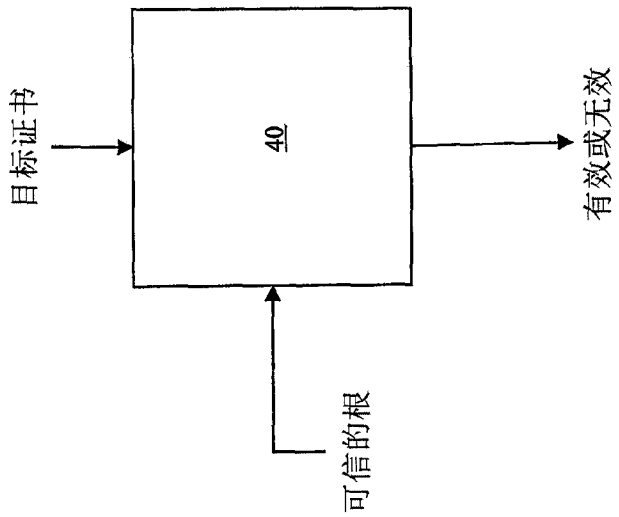

图 2

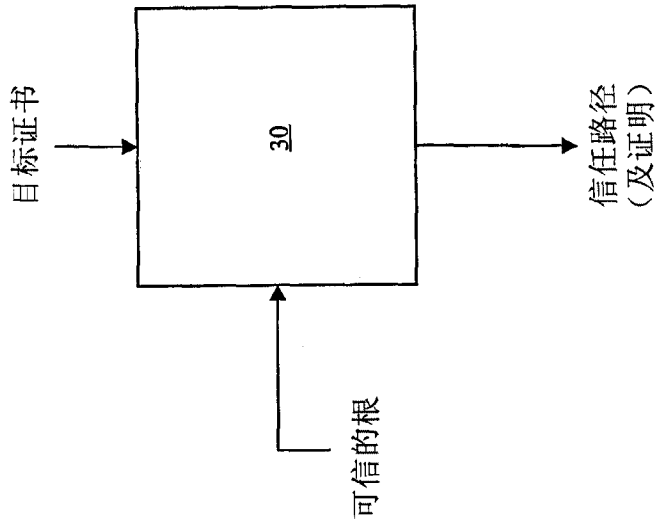

图 1

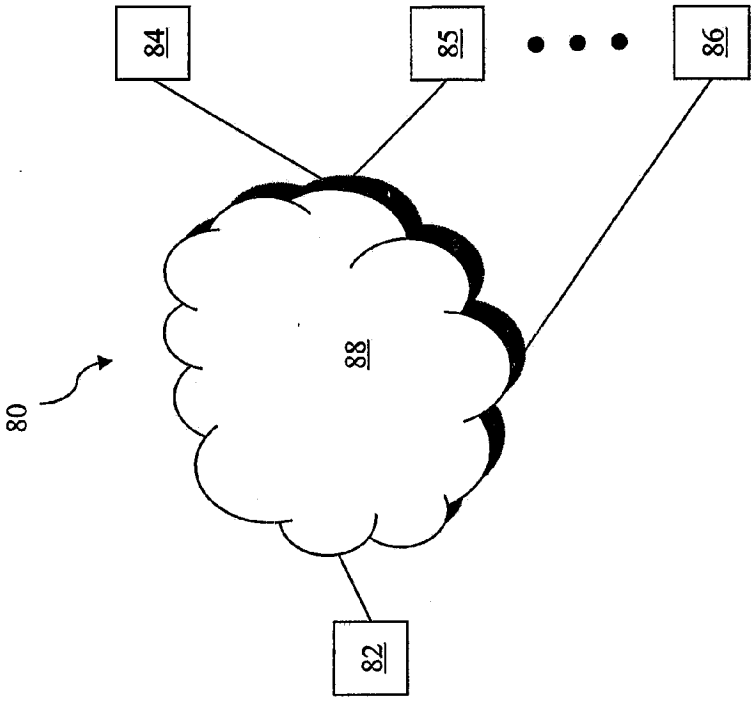

图 4

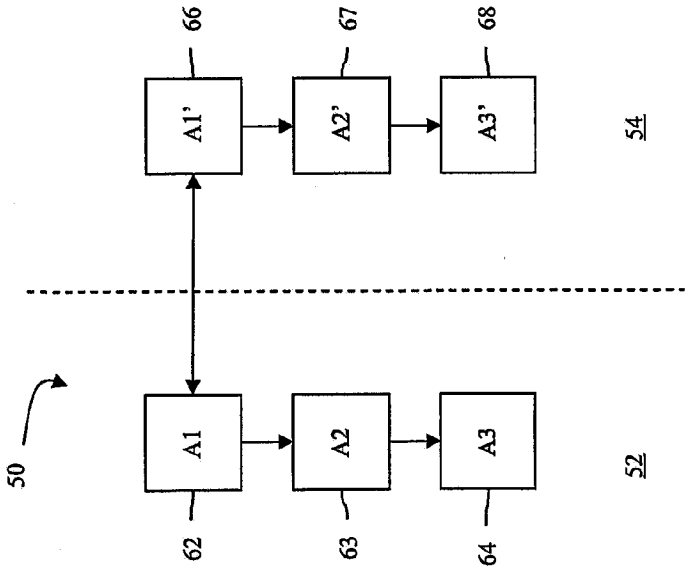

图 3

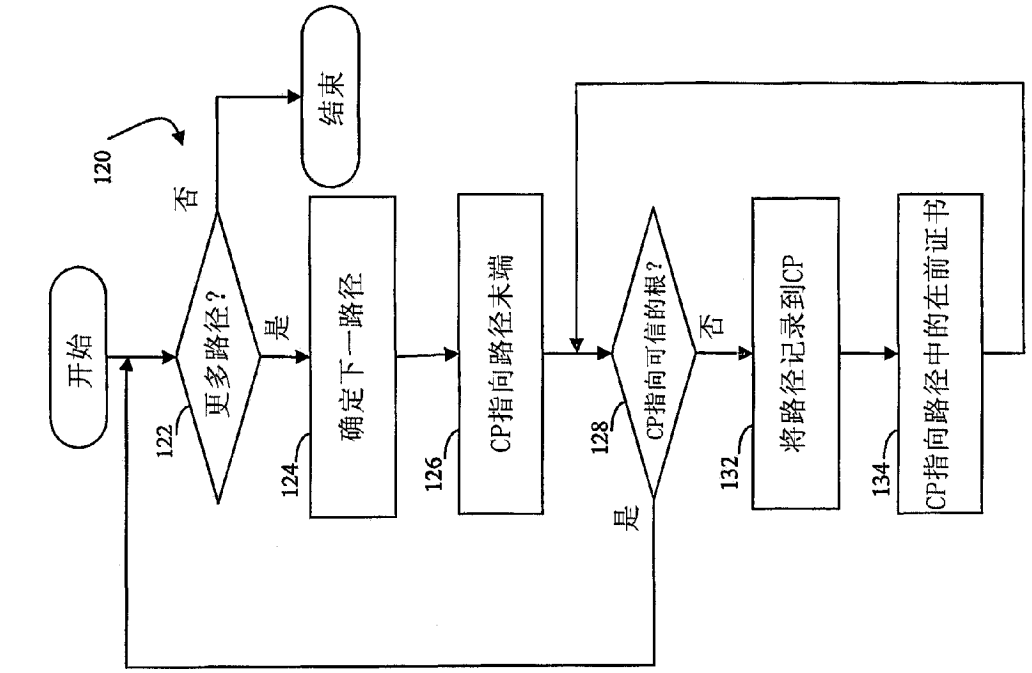
开始
更多路径?
120
122
否
是
结束
确定下一路径
124
CP指向路径末端
126
CP指向可信的根?
128
否
是
将路径记录到CP
132
CP指向路径中的在前证书
134

图 6

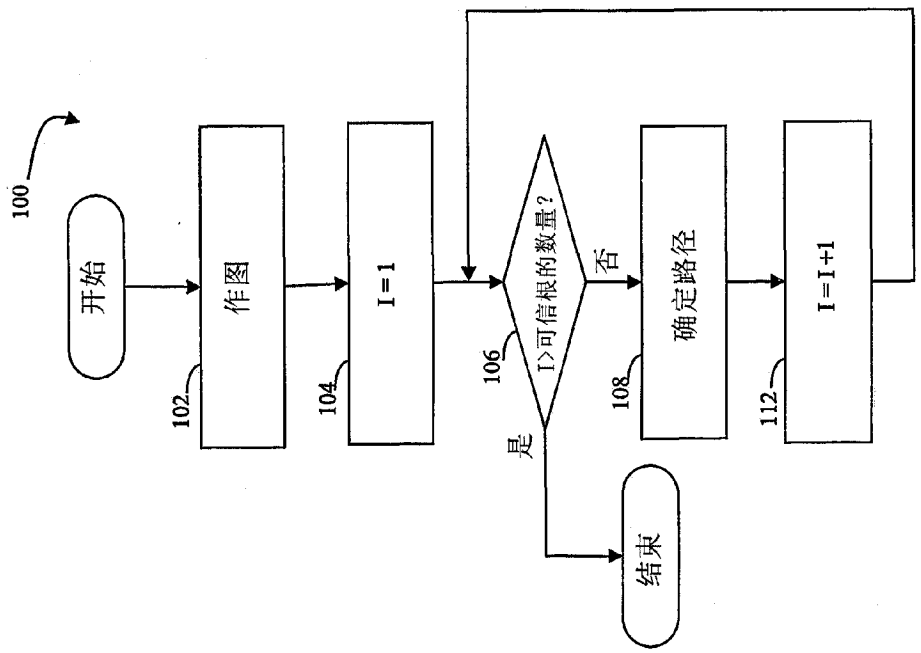
100
开始
作图
102
I = 1
104
I>可信根的数量?
106
否
是
确定路径
108
I = I +1
112
结束

图 5

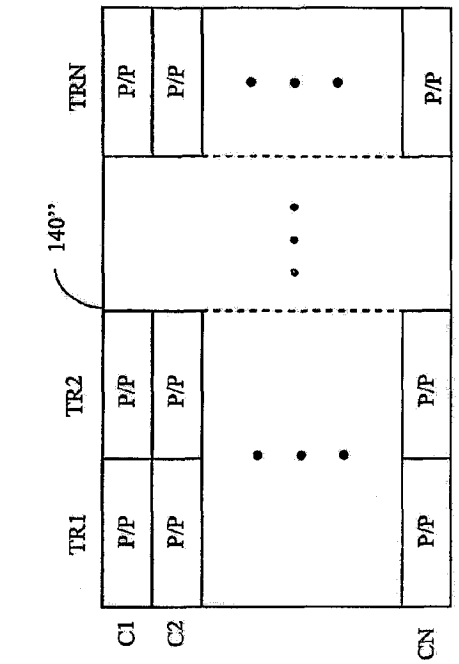
140''
TRN
TR2
TR1
P/P
C1
C2
CN

图 7C

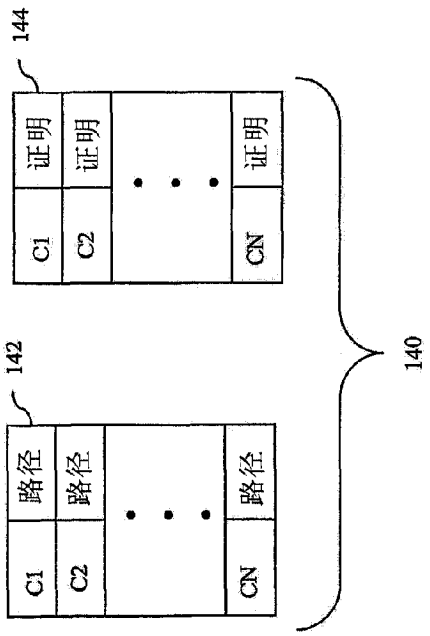
144
142
140
证明
路径
C1
C2
CN

图 7A

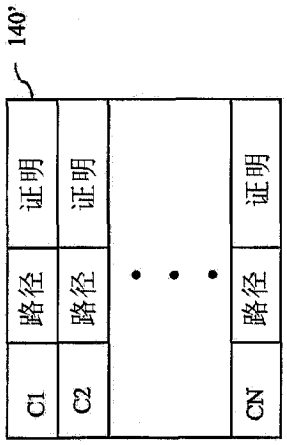
140'
证明
路径
C1
C2
CN

图 7B

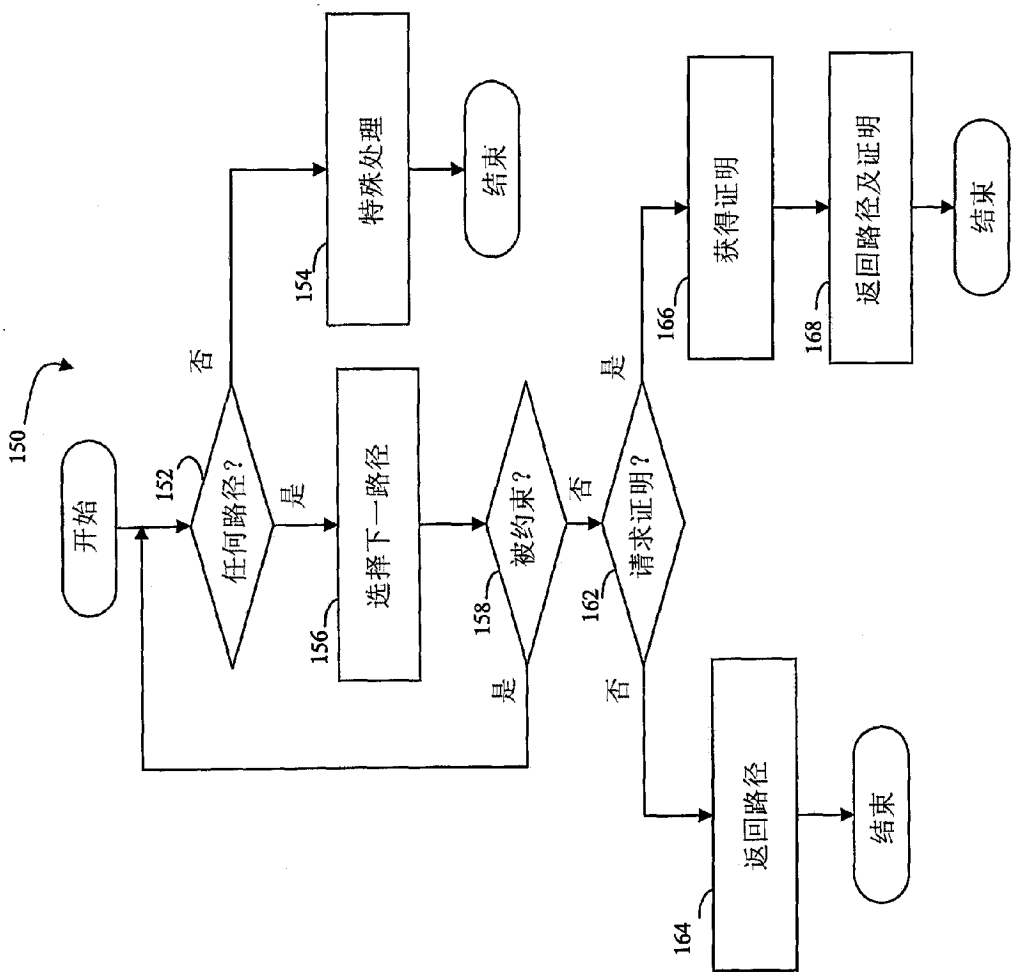
150
开始
152
任何路径?
否
是
154
特殊处理
结束
156
选择下一路径
158
被约束?
是
否
162
请求证明?
是
166
获得证明
168
返回路径及证明
结束
否
164
返回路径
结束

图 8

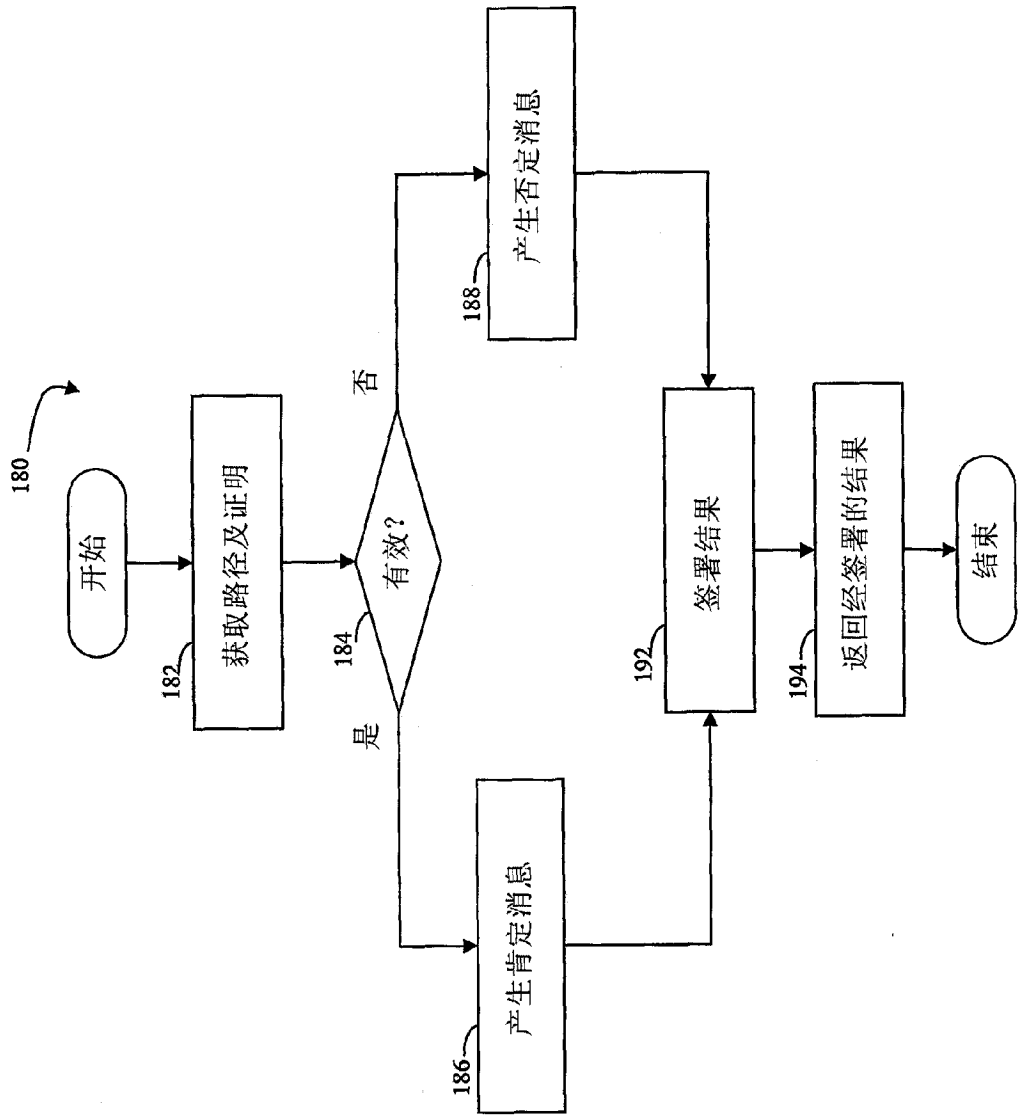
180
开始
182
获取路径及证明
184
有效?
否
是
188
产生否定消息
186
产生肯定消息
192
签署结果
194
返回经签署的结果
结束

图 9