

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷

G06F 15/163

H04L 9/30 G07F 19/00

[12] 发明专利申请公开说明书

[21] 申请号 00132818.2

[43] 公开日 2001 年 7 月 25 日

[11] 公开号 CN 1305159A

[22] 申请日 2000.11.1 [21] 申请号 00132818.2

[30] 优先权

[32] 1999.11.1 [33] US [31] 60/162,673

[71] 申请人 城市集团发展中心有限公司

地址 美国加利福尼亚州

[72] 发明人 约翰·莱纳斯·施威帕

马克·沙利文

[74] 专利代理机构 隆天国际专利商标代理有限公司

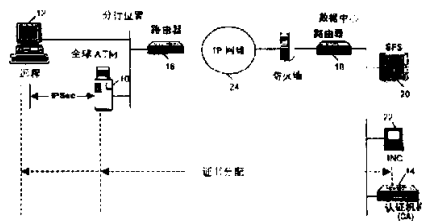
代理人 陈红 潘培坤

权利要求书 5 页 说明书 27 页 附图页数 12 页

[54] 发明名称 用于自助金融交易终端的安全通信的方法和系统

[57] 摘要

一种用于通过网络在银行业务节点之间进行安全通信的方法和系统,利用运行在银行业务节点使用的平台(如 NT 操作系统平台)上的因特网协议安全性(IPSec)软件客户程序,提供一个银行业务节点(如一个 ATM)与另一个银行业务节点(如一个远程操作员接口),一个主机和/或一个外部系统管理节点之间的端对端安全性。认证机构处理从 ATM 网络上参与端对端安全性的银行业务节点引入的认证请求。



ISSN 1008-4274

权 利 要 求 书

1. 一种用于通过网络在银行业务节点之间进行安全通信的方法，其特征在于包括：

5 在网络上的至少一个银行业务节点上安装用于认证授权的根认证证书；

通过网络将银行业务节点的一个带有公用密钥的认证请求发送到认证机构；

10 通过网络向银行业务节点发送一个数字认证证书，通过认证机构证实银行业务节点的身份；以及

通过交换该银行业务节点的数字认证证书和另一个银行业务节点的数字认证证书，允许该银行业务节点与网络上至少另一个银行业务节点相互证实身份。

15 2. 如权利要求 1 所述的方法，其特征在于在银行业务节点上安装根认证证书的步骤还包括在银行业务节点上安装一个用于认证当局的自签名的数字认证证书。

3. 如权利要求 1 所述的方法，其特征在于在银行业务节点上安装根认证证书的步骤还包括在银行业务节点上采用基于软盘的安装、基于网络的安装、和基于仓库的安装中的一种方法来分配根认证证书。

20 4. 如权利要求 1 所述的方法，其特征在于在银行业务节点上安装根认证证书的步骤还包括在自助交易终端节点、远程操作员接口节点、主机节点、和一个外部系统管理节点中的一个上安装根认证证书。

5. 如权利要求 1 所述的方法，其特征在于在银行业务节点上安装根认证证书的步骤还包括接收输入的用于通过银行业务节点进行认证授权的
25 IP 地址。

6. 如权利要求 5 所述的方法, 其特征在于接收输入的用于认证授权的 IP 地址还包括提示输入用于认证机构的 IP 地址。

7. 如权利要求 1 所述的方法, 其特征在于在银行业务节点上安装根认证证书的步骤还包括接收输入的用于至少另一个被指定用来管理该银行业务节点的银行业务节点的 IP 地址。

8. 如权利要求 7 所述的方法, 其特征在于接收输入的用于另一个银行业务节点的 IP 地址还包括提示输入另一个银行业务节点的 IP 地址。

9. 如权利要求 1 所述的方法, 其特征在于发送认证请求还包括通过网络将一个带有公用密钥的认证请求发送到以 IP 地址配置的认证机构。

10. 如权利要求 1 所述的方法, 其特征在于发送认证请求还包括生成用于该银行业务节点的认证请求和一个公用/私有密钥对。

11. 如权利要求 10 所述的方法, 其特征在于生成公用/私有密钥对还包括在本地将私有密钥存储到银行业务节点上。

12. 如权利要求 1 所述的方法, 其特征在于发送认证请求还包括发送带有用于识别该银行业务节点的信息的认证请求。

13. 如权利要求 1 所述的方法, 其特征在于发送数字认证证书还包括通过认证机构发出用于确认该银行业务节点身份的数字认证证书。

14. 如权利要求 13 所述的方法, 其特征在于发出数字认证证书还包括: 检查允许认证机构确认的银行业务节点的认证机构的策略数据库。

15. 如权利要求 14 所述的方法, 其特征在于检查策略数据库还包括: 更新策略数据库以反映出向银行业务节点发出了数字认证证书。

16. 如权利要求 13 所述的方法, 其特征在于发出数字认证证书还包括将该银行业务节点加入到由允许认证机构确认的银行业务节点构成的认证机构的策略数据库中。

17. 如权利要求 16 所述的方法, 其特征在于将银行业务节点加入到策

略数据库中还包括通过专用的策略数据库管理工具将银行业务节点加入到策略数据库中。

18. 如权利要求 17 所述的方法, 其特征在于通过专用的策略数据库管理工具将银行业务节点加入到策略数据库中还包括: 提示用户通过策略数据库管理工具的一个图形用户接口输入该银行业务节点的 IP 地址。

19. 如权利要求 1 所述的方法, 其特征在于发送数字认证证书还包括将数字认证证书引入到银行业务节点的 IPSec 配置中。

20. 如权利要求 1 所述的方法, 其特征在于允许银行业务节点相互证实身份还包括根据各自的数字认证证书, 通过各自银行业务节点的 IPSec 配置, 来证实各银行业务节点的身份。

21. 一种用于通过网络在银行业务节点之间进行安全通信的系统, 包括:

用于在网络上的至少一个银行业务节点上安装用于认证机构的根认证证书的装置;

用于通过网络将一个银行业务节点的带有公用密钥的认证请求发送到认证机构的装置;

用于通过网络向银行业务节点发送一个数字认证证书以便通过认证机构来证实银行业务节点的身份的装置; 以及

用于通过交换该银行业务节点的数字认证证书和另一个银行业务节点的数字认证证书, 允许该银行业务节点与网络上至少另一个银行业务节点相互证实身份的装置。

22. 如权利要求 21 所述的系统, 其特征在于用于在银行业务节点上安装根认证证书的装置还包括用于在银行业务节点上安装一个用于认证机构的自签名的数字认证证书的装置。

23. 如权利要求 21 所述的系统, 其特征在于用于在银行业务节点上安

装根认证证书的装置还包括用于在银行业务节点上采用基于软盘的安
装、基于网络的安装、和基于仓库的安装中的一种来分配根认证证书的装
置。

24. 如权利要求 21 所述的系统,其特征不在于用于在银行业务节点上安
5 装根认证证书的装置还包括用于在自助交易终端节点、远程操作员接口节
点、主机节点、和一个外部系统管理节点中的一个上安装根认证证书的装
置。

25. 如权利要求 21 所述的系统,其特征不在于用于在银行业务节点上安
装根认证证书的装置还包括用于接收输入的用于银行业务节点的认证机
10 构的 IP 地址的装置。

26. 如权利要求 25 所述的系统,其特征不在于用于接收输入的认证机构
的 IP 地址的装置还包括用于提示认证机构的 IP 地址的装置。

27. 如权利要求 21 所述的系统,其特征不在于用于在银行业务节点上安
装根认证证书的装置还包括用于接收输入的用于至少另一个被指定用来
15 管理该银行业务节点的银行业务节点的 IP 地址的装置。

28. 如权利要求 27 所述的系统,其特征不在于用于接收输入的用于另一
个银行业务节点的 IP 地址的装置还包括用于提示另一个银行业务节点的
IP 地址的装置。

29. 如权利要求 21 所述的系统,其特征不在于用于发送认证请求的装置
20 还包括用于通过网络将带有公用密钥的认证请求发送到配置有一个 IP 地
址的认证机构的装置。

30. 如权利要求 21 所述的系统,其特征不在于用于发送认证请求的装置还
包括用于生成该银行业务节点的认证请求和一个公用/私有密钥对的装置。

31. 如权利要求 30 所述的系统,其特征不在于用于生成公用/私有密钥
25 对的装置还包括用于在本地将私有密钥存储到银行业务节点上的装置。

32. 如权利要求 21 所述的系统, 其特征在于用于发送认证请求的装置还包括用于发送带有用于识别该银行业务节点的信息的认证请求的装置。

33. 如权利要求 21 所述的系统, 其特征在于用于发送数字认证证书的装置还包括用于发出通过认证机构确认该银行业务节点的身份的数字认证证书的装置。

34. 如权利要求 33 所述的系统, 其特征在于用于发出数字认证证书的装置还包括用于检查银行业务节点的允许认证机构确认的认证机构的策略数据库的装置。

35. 如权利要求 34 所述的系统, 其特征在于用于检查策略数据库的装置还包括用于更新策略数据库以反映出向银行业务节点发出了数字认证证书的装置。

36. 如权利要求 33 所述的系统, 其特征在于用于发出数字认证证书的装置还包括用于将该银行业务节点加入到由允许认证机构确认的银行业务节点构成的认证机构的策略数据库中的装置。

37. 如权利要求 36 所述的系统, 其特征在于用于将银行业务节点加入到策略数据库中的装置还包括用于通过专用的策略数据库管理工具, 将银行业务节点加入到策略数据库中的装置。

38. 如权利要求 37 所述的系统, 其特征在于通过专用的策略数据库管理工具将银行业务节点加入到策略数据库中的装置还包括提示用户通过策略数据库管理工具的一个图形用户接口输入该银行业务节点的 IP 地址。

39. 如权利要求 21 所述的系统, 其特征在于发送数字认证证书的装置还包括将数字认证证书引入到银行业务节点的 IPsec 配置中。

40. 如权利要求 21 所述的系统, 其特征在于允许银行业务节点相互证实身份的装置还包括根据各自的数字认证证书, 通过各自银行业务节点的 IPsec 配置, 来证实各银行业务节点的身份的装置。

说明书

用于自助金融交易终端的安全通信的方法和系统

5 本发明一般涉及自助金融交易终端领域，例如自动出纳机(ATMs)，具体涉及一种用于 ATM 和诸如远程终端之类的远程操作员接口之间的安全通信的方法和系统。

ATM 机器包括计算机应用程序或在 ATM 机内的计算机硬件运行的软件，ATM 机例如与经网络连接到 ATM 的一个主计算机和其他远程计算机接口。对于拥有和/或管理并维护 ATM 机的机构，确保经其 ATM 网络的数据通信的安全是极其重要的，该机构一般是一个诸如银行之类的金融机构。当前，还没有令金融机构能够保证其 ATM 网络上的端对端的安全、并使金融机构能够可靠地管理通过 ATM 网络的数据的满意措施。

15 本发明的一个特征和优点是提供用于一个诸如一 ATM 之类的自助交易终端和一个诸如远程 PC，主计算机，或主网络监视器之类的远程操作员接口之间的安全通信的方法和系统。

本发明的另一个特征和优点是提供用于一个自助交易终端和一个远程操作员接口之间的安全通信的方法和系统，该方法和系统保证通信的端对端加密。

20 本发明的进一步的特征和优点是提供用于自助交易终端和一个远程操作员接口之间的安全通信的方法和系统，其中加密和安全性对远程操作员接口客户是透明的。

本发明的附加特征和优点是提供用于一个自助交易终端和一个远程操作员接口之间的安全通信的方法和系统，该方法和系统使用自动生成的非对称密钥和认证。

本发明的再一个特征和优点是提供用于一个自助交易终端和一个远程操作员接口之间的安全通信的方法和系统,该方法和系统包括自动安装特征。

为实现上述和其他特征,优点和目的,本发明的一个实施例使用在诸如 NT 操作系统平台之类的平台上运行的,用于银行业务节点的因特网协议安全性 (IPSec) 软件客户程序,提供一个诸如 ATM 之类的一个银行业务节点和一个诸如远程操作员接口,主机,或一个外部系统管理节点之类的另一个银行业务节点之间的端对端安全性。本发明的一个实施例使用基于一种方法的非对称密钥或认证的一种方法,该方法涉及在配置时自动生成一个公用和私有密钥对的银行业务节点,并且当进行密钥生成时把一个认证请求放在一起。认证机构处理从参与端对端安全性的 ATM 网络上的银行业务节点输入的认证请求。本发明的一个实施例还包括自动安装方面。

本发明的一个实施例通过配置通过使用程序 IPSec 的安全隧道传送的节点之间的所有网络通信,保证经 ATM 网络的银行业务节点之间的安全通信。在本发明的一个实施例中,例如,在一个 ATM 和/或诸如远程操作员接口节点,主机节点之类的用于保证安全通信的任何其他银行业务节点,和/或外部系统管理节点安装一个根认证证书,该根认证证书是认证机构的自-签名数字认证证书证书。例如,可以将根认证证书用于基于软盘的安装,基于网站的安装,或基于库房的安装。在安装过程中,输入 IP 地址用于认证机构和一个或多个其他银行业务节点,例如为管理特定的 ATM 指定的另一个银行业务节点。

在配置根认证证书时,在本发明一个实施例中,银行业务节点产生一个认证请求和用于该银行业务节点的一个公用/私有密钥对,将私有密钥本地存储在该银行业务节点,并将与公用密钥打包在一起的认证请求经网络发送到配置了一个 IP 地址的认证机构。该认证请求和公用密钥与识别

该银行业务节点的信息一起被发送到认证机构。在接收该认证请求时，认证机构检查用于银行业务节点的该认证机构的策略数据库，该策略数据库允许该认证机构进行鉴别。如果在该策略数据库找到请求该认证的银行业务节点，则认证机构发出鉴别该银行业务节点身份的数字认证证书证书。

5 在本发明一个实施例中，认证机构将数字认证证书证书经证明银行业务节点身份的网络发送到请求银行业务节点并更新策略数据库以反映数字认证证书证书到银行业务节点的发送。为使一个数字认证证书发送到请求银行业务节点，该特定的银行业务节点必须处于该认证机构的策略数据库，该策略数据库由允许认证机构进行鉴别的银行业务节点组成。通过点
10 击显示在管理工具的图形用户接口的显示屏上的‘加入一个节点’并响应提示输入该银行业务节点的 IP 地址，经专用的策略数据库管理工具执行将一个银行业务节点增加到该策略数据库。

在本发明的一个实施例中，将认证机构发出的数字认证证书输入请求银行业务节点的 IPSec 配置，并且通过各个银行业务节点的数字认证证
15 书的交换允许诸如 ATM 之类的银行业务节点与至少一个诸如远程操作员接口，主机接口，和/或外部系统管理节点之类的其他银行业务节点相互检验识别。根据通过每个银行业务节点的 IPSec 配置的相应的数字认证证书通过检验两个银行业务节点的身份执行相互检验。

本发明的附加目的，优点，以及新颖特征在后面的详细描述中部分列
20 出，并且对本领域技术人员来说，通过下面的，或实施本发明所得到的理解，本发明的附加目的，优点，以及新颖特征将变得显而易见。

图 1 是表示用于本发明一个实施例的一个方面的密钥组件的实例的示意图以及密钥组件之间的信息流的示意图。

图 2 是表示用于本发明的一个实施例的另一个方面的密钥组件的实
25 例的示意图以及用于安全隧道的密钥组件之间的信息流的示意图。

图 3 是表示用于本发明的一个实施例的密钥组件的实例的示意图以及用于阻断未认证的节点的密钥组件之间的信息流的示意图。

图 4 是表示用于本发明的一个实施例的密钥组件的实例的示意图以及用于认证交换的密钥组件之间的信息流的示意图。

5 图 5 是表示用于本发明的一个实施例的密钥组件的实例的示意图以及用于根认证证书配置的密钥组件之间的信息流的示意图。

图 6 是表示用于本发明的一个实施例的密钥组件的实例的示意图以及用于认证获得的密钥组件之间的信息流的示意图。

图 7 是表示用于本发明的一个实施例的 IPSec 的配置参数的实例以及
10 所选择的如何设定这些参数的实例的表。

图 8 是表示用于本发明一个实施例的必须允许以便支持安全通信的端口和协议以及远程操作员接口功能性的实例的表。

图 9 是用于本发明实施例的 ‘CA 数据库维护工具’ 的简单的图形用户接口 (GUI) 屏幕。

15 图 10 是用于本发明实施例的 GMT 的使用实例的示意图图。

图 11 是用于本发明一个实施例的其中认证对该认证节点无效的情况的实例的示意图；和

图 12 是用于本发明一个实施例的其中认证对其他节点无效的情况的实例的示意图。

20 现在详细参照本发明的一个实施例，在附图中表示的实例，图 1 是表示用于本发明的一个实施例的一个方面的密钥组件的实例的示意图以及密钥组件之间的信息流的示意图。本发明的一个实施例的方法和系统使用基于因特网协议安全性 (IPSec) 的解决方案提供 ATM10 和远程操作员接口 12 之间的端对端的安全性，该基于因特网协议安全性的解决方案在很
25 大程度上是 “传输控制协议/因特网协议 (TCP/IP) “数据通信安全性。

本发明的一个实施例使用在诸如 Windows NT 平台之类的平台上运行的 IPSec 软件客户程序。一种适用于 IPSec 软件客户程序的实例是一个由一个公司提供的被称为 IRE 的产品。

在本发明的一个实施例的这一方面，在被称为 ATM 或全球 ATM10 的 ATM 机上使用在 NT 平台运行的 IPSec 软件客户程序。全球 ATM10 设置一个由工作人员使用的用户触摸点 12，该用户触摸点与位于 ATM10 前面的常规的客户触摸点分开。具体地说，用户触摸点 12 与 ATM 本身分开并采用运行一个网络浏览器的个人计算机（PC）12 的形式。当工作人员按照获得的状态信息操作 ATM10 或校验 ATM10 时，或者如果一个作为银行业务工作人员的现场工程师希望维护并诊断 ATM10 的问题，他或她使用远程操作员接口 PC12 的远程浏览器。远程操作员接口 PC12 的位置一般处于与 ATM 相同的房间或者位于附近的工作人员房间。然而，远程操作员接口 PC12 可以延伸到任何位置。

在本发明的一个实施例中，由远程操作员接口的工作人员使用的客户 PC12 被称为远程操作员接口触摸点。该远程操作员接口触摸点 12 由一个运行诸如 Windows NT 之类的操作系统的 PC 平台组成。出于安全的原因，诸如 Windows NT 之类的操作系统运行在平台上以提供一个安全的操作系统环境。与操作系统一起，还有诸如 Internet Explorer 4.0 版本或更高版本之类的浏览器也运行在远程操作员接口 PC12。作为本文的一个实例，在远程操作者机 12 和 ATM 或全球 ATM10 之间提供安全通信的特征是基于 IPSec 的软件，诸如被称为 SafeNet/Soft-PK 的 IRE 产品，IPSec 不但安装在远程操作者机 12 而且安装在 ATM 或全球 ATM10。

例如，可以以两种方式配置 IPSec 软件，以便可得到用于本发明的一个实施例的安全通信。一种方式是使用远程操作者机 12 和全球 ATM10 之间的被称为预共享密钥的配置。考虑使用预共享密钥方法的一个原因是该

方法提供一种管理 ATM 网络 24 内的节点之间的加密的简单方式。然而，使用预共享密钥具有一个潜在的问题，即，例如由于远程操作者机 12 上的未授权用户设法进入这种配置并掌握预共享密钥或加密，从而危及预共享密钥技术的安全。配置 IPsec 软件的另一个方式是使用非对称密钥方法，或者被称为基于认证证书的方法，在 IPsec 标准中也支持这种方法。该方法涉及诸如 ATM10 之类的客户机，产生在配置时设定的密钥对。该客户机产生公用和私有密钥对，并且同时，在密钥生成时和认证请求放在一起。从这里，将认证请求发送到认证机构 14，将认证机构 14 设计在银行业务基础结构内。

认证机构 14 是另一个基于 PC 的机器，该机器运行例如一个诸如具有因特网信息服务器的 Windows NT Server 之类的网络服务器，以及，例如一个微软认证服务器产品。该认证服务器产品处理从银行业务节点输入的请求，该银行业务节点包括诸如 ATM10 之类的全球 ATM，以及诸如 PC12 之类的远程操作员接口机，并且还可以包括参与端对端解决方案的沿着网络 24 的路由器 16 和 18 之类的部件。另外，也设置其他端节点以用于安全通信。例如，金融机构的前端金融主机 20 运行 IPsec，以及金融机构的网络分布系统，前端金融主机 20 是一个提供软件分布业务以及监控 ATM 网络 24 内的所有 ATM 的智能网络控制器 22。现场服务人员或银行工作人员使用远程操作员接口客户程序 12 来了解关于 IPsec 安全的解决方案的任何事情是不必要的，该方案不但对用户透明，而且对于被开发用于两个节点的预存程序透明。本发明的一个实施例使用在 IP 层实施的加密和安全性，该 IP 层为透明层，并且这种加密和安全性提供一种保证端对端加密的非常简单的方式。

本发明的一个独特方面是向诸如 ATM10 之类的全球 ATM 提出一种特殊的要求，该全球 ATM 是远程服务的，并且可以几乎完全自动地进行安装的

机器。特定类型的 ATM10 没有键盘和鼠标，并且，与本发明这一方面相关的一个重要特征是能够以自动的方式安装和配置 IPSec 软件。因此，这一方面采用诸如 IRE SafeNet/Soft-PK 之类的 IPSec 客户软件产品，并创建一个对所有自动安装均有正确响应的内部打包的无声安装脚本。

5 另外，在本发明实施例的这一方面还存在其他特征，例如以自动方式产生非对称密钥的性能，该性能还包括认证请求，该认证请求是由一个特定的客户软件集进行的。一种以自动方式产生非对称密钥的方式是使其成为原稿，或包括成为原稿的与认证生成系统一起的命令行的变量。另一个方法使用诸如被称为 Microsoft Test 的微软产品之类的产品，该产品自
10 动执行所有适当的击键动作，就好象安装者正在按下键盘上的键一样。按此方法，创建 Microsoft Test 脚本，该脚本自动产生密钥并产生一个认证请求。

 在产生认证请求之后，将该认证请求发送到认证服务器 14。从这里，在认证服务器一侧，客户策略模块从诸如 ATM10 或金融机构的远程操作
15 员接口机 12 之类的金融机构的银行业务节点接收认证请求。驻留在认证服务器 14 的策略模块从预认证银行业务节点的数据库开始工作，该数据库主要由节点名称和 IP 地址组成。策略模块将认证请求与数据库进行比较，并且该策略模块处理该请求，以此作为数据库内的请求银行业务节点，并将实际认证证书发回诸如 ATM10 或远程操作员接口 PC12 之类的请
20 求银行业务节点。当认证证书从认证服务器 14 返回到银行业务节点时，自动接收所产生的认证证书并将其安装在 IPSec 软件，以便可以操作。根据认证配置，要求从认证服务器得到该认证证书并将其安装在 IPSec 客户软件内或在其内实施。在完成上述过程并将认证证书安装在客户程序之后，金融机构能够进行安全通信。

25 因为将 IPSec 客户程序配置在一个端节点，本发明的一个实施例的这

一方面的另一个特征，是创建该特定节点的策略定义。其含义是在特定端点能够定义例如全球 ATM10，使全球 ATM10 能在另一个端点进行安全通信。在全球 ATM10 的情况下，全球 ATM 必须与例如一个特定的远程操作员接口机 12 通信。因此，全球 ATM10 要建立策略定义，表明全球 ATM10 5 必须与特定的远程操作员接口机 12 进行安全通信。在该策略定义中通过诸如 IP 地址和不同的名称之类的各种参数定义远程操作员接口机 12。处于全球 ATM10 上的策略定义保证其本身与远程操作员接口机 12 之间的安全通信。全球 ATM 与其通信的任何其他节点在该机器上也建立策略定义以允许安全通信，该机器包括，例如，一个作为用于银行业务系统的主网络 10 监视器的 ATM 监控和管理机器 22，和一个其上具有所有客户交易数据的金融机构的前端金融主机 20。

在这一方面，就将 IPsec 认为是一个新出现的加密标准而言，出现这样的问题，即，关于如何完成例如全球 ATM12 和主网络监视器 22 之间和/或全球 ATM12 和前端主机 20 之间的端对端的安全性。为解决该问题， 15 在主网络监视器 22 和前端主机 20 的前面设置一个诸如 Cisco 路由器之类的的路由器。例如，路由器 18 直接位于主网络监视器 22 的前面，并且全球 ATM12 和路由器 18 之间为安全通信。按本发明的另一个特征，IPsec 客户软件运行在主网络监视器机 22 上，并且在 IPsec 客户软件实际安装在主网络监视器机 22 之前保证主网络监视器机 22 上的金融机构的预存软件 20 的操作性是很重要的。对于低风险的方法，将路由器 18 配置在主网络监视器机 22 的前面以提供安全的端对端通信。

本发明的这一方面的一个重要特征是支持安全的端对端通信的 IPsec 解决方案在全球 ATM10 上的自动安装。该 IPS 解决方案使用与 IPsec 兼容的预存软件，并且本发明的一个实施例包括使用 IPsec 的自动化特 25 征，该 IPsec 通过使用写入客户策略模块主要实施在全球 ATM10 并且部

分实施在金融机构的认证服务器机 14。根据远程操作员接口机 12，用于常规的情况，例如，配置 IPSec 客户软件键盘，鼠标和指令。

在本发明一个实施例中进行的安全通信类型是加密数据，并且 IPSec 列出关于加密数据后面的机构的所有细节。在应用程序层，被交换的数据包括例如调节帐户和调节 ATM 机上的货币。然而，对于本发明的一个实施例所实施的安全性在一个较低的层面上进行，该层称为因特网协议（IP）层。除了所要保护的敏感数据处于应用程序层的情况之外，应用程序层和 IP 层不关联，并且在较低层保证或保护该数据。

本发明在这一方面使用 IPSec 的期望特征是这一使用是在内部网和因特网通信的公用点进行的。实际上所有的数据通信现在或将来要通过传输控制协议/因特网协议（TCP/IP）运行的，该传输控制协议/因特网协议是一个其中提供加密解决方案的公用层。如果该加密解决方案被设置得太高，设置在应用程序层，则其成为专用于一个特定的应用程序。如果设置得太低，例如在链接层，则依靠硬件规定，例如令牌环或以太网。加密解决方案在 IP 层上的实施与例如在银行业务网络 24 内，在因特网上，以及在多数公司内部网上的多数数据通信量通过的多数一般的通信点一致。

图 2 是表示用于本发明一个实施例的另一个方面的密钥组件的实例的示意图以及用于安全隧道的密钥组件之间的信息流的示意图。在这一方面，一个全球 ATM 网络安全实施方案在全球 ATM10 和远程操作员接口 12 或 26 之间提供一个完全加密并确认的网络路径，就好象其通过虚拟专用网络（VPN）、微通道结构（MCA）、图形程序设计接口（GPI）、以及图形互换格式（GIF）版本传送一样。另外，该实施方案的一个特征是保证从全局 ATM10 到外部系统管理部分 22 和从全球 ATM10 到主机 20 的网络路径，这样就提供一种用于实现全球 ATM 环境的完全加密和确认的端对端

网络的解决方案。

在这一方面，为提供用于全球 ATM 操作环境的网络安全性，在全球 ATM10 和远程操作员接口 12 或 26 之间的所有网络通信量都要经过确认和加密。这通过配置这些网络节点之间的通信量以通过一个诸如安全隧道 30 或 32 之类的安全隧道来实现上述加密和确认。一个隧道是两个或多个机器之间的虚拟连接，通过加密和确认，该隧道保证通信各方的身份和通信的完全保密性和完整性。网络 24 上的另一个机器不能看到正通过该隧道的数据。从技术上说，它们可以看到数据流动，但是它们不能解密数据，因此该数据实际上为无法理解的。不能影响高效通过该隧道的数据，也不能模拟该隧道端点。该技术被称为虚拟专用网；完全是为了实施，它在极少的专用网络内或者甚至在公用的网络内创建一个极端专用的虚拟网络。

在全球 ATM 实施方案的这一方面，所有隧道都是唯一的。一个给定的隧道仅用于两个机器之间，例如全球 ATM10 和远程操作员接口机 12 之间的隧道 30。如果存在与特定的全球 ATM 通信的另一个远程操作员接口机，例如 PC26，则存在与该通信相关的不同的隧道 32。如果一个远程操作员接口机与多于一个的全球 ATM 通信，则也是这种情况。该远程操作员接口机具有用于每个全球 ATM 的唯一隧道，通过该隧道每个全球 ATM 与远程操作员接口机接触。

另外，在这一方面，直接连接诸如主机 20 和外部系统管理部件 22 之类的其他节点和全球 ATM 的网络。未明显允许与全球 ATM10 通信的网络节点被阻断在网络层。图 3 是表示用于本发明一个实施例的密钥组件的实例的示意图以及用于未认证节点 34 的阻断的密钥组件之间的信息流的示意图。用于本发明这一方面的网络安全性实施方案的另一个特征涉及到与全球 ATM10 通信的所有网络节点和来自所述节点的确认和加密。

选择用于本发明这一方面的安全性解决方案是因特网协议安全性 (IPSec) 的一种实施方案。该实施方案加强了在网络层提供加密和确认业务的 IP 协议, 因此所有较高层可以透明地利用这些业务。通过将 IPSec 布置在两个或多个机器并适当地进行配置, 这些机器之间的所有基于 IP 的网络通信量都得到了加密和确认, 完全不用了解使用网络连接性的较高级应用程序。IPSec 是一种基于标准的解决方案, 该方案很快成为对于因特网联网安全性的实施方案以及虚拟专用网络的创建的一种选择技术。一个适用于本发明实施例的 IPSec 数据包应该是稳定的、具有优良的安全性特征、易于配置、并与诸如 IRE Inc 的 SafeNet/Soft-PK 之类的硬件制造兼容的、用于 IPSec 的扩展交叉认证。

在这一方面, 当建立用于本发明实施例的两个或多个网络节点之间的安全通信时, IPSec 必须检验节点的身份。IPSec 使用两个不同的确认方法, 它们是: 预共享密钥和 X.509v3 数字认证证书。预共享密钥模块使用共享加密以证明概念上和一个口令类似的身份。这本质上具有较小安全性并基本上比数字认证证书模块更难于管理, 在数字认证证书中由一个可信的第三方提供确认。数字认证证书具有支持非否认的附加优点。

因此, 在本发明的这一方面, X.509v3 数字认证证书用于提供全球 ATM 和远程操作员接口节点的身份的确认。图 4 是表示用于本发明一个实施例的密钥组件的实例的示意图以及用于认证交换的密钥组件之间的信息流的示意图。这些认证证书 36, 38 用于节点 10 和 12 之间的安全隧道的建立。具体地说, 节点 10 和 12 交换其认证证书 36 和 38, 因此它们中的每一个都在其中的检验另一个的身份。对认证证书 36, 38 进行密码检验, 在这点上保证身份并建立安全隧道。

在本发明的这一方面, 认证机构 (CA) 14 发出确认全球 ATM10 和远程操作员接口节点 12、26 的身份的数字认证证书。CA14 作为可信的第三

方，驻留在被保护的数据中心或其他的安全机构内，并且可由可信数据中心人员进行管理。CA14 包含要进行确认的节点列表，该节点列表被称为策略数据库。当新的节点放置在网络 24 上时，数据中心人员必须更新策略数据库。否则，CA14 将不确认新节点。未被确认的节点不能建立与其他节点的安全通信。全球 ATM10 不允许其本身和远程操作员接口 12 或 26 之间的不安全通信。用于本发明一个实施例的适用的 CA14 应该是可扩展的，与操作系统集成在一起，易于配置和管理，并具有较高可配置安全性实施方案，例如微软的认证服务器。

图 5 是表示用于本发明的一个实施例的密钥组件的实例的示意图以及用于根认证证书配置的密钥组件之间的信息流的示意图。在这一方面，必须建立一个诸如远程操作员接口 12 或全球 ATM10 之类的节点和 CA14 之间的信任关系，以使该节点可以使用由特定的 CA14 发出的身份认证证书。这可以通过在该节点 10 或 12 安装 CA 的自签名数字认证证书或根认证证书 40 实现。一旦完成该过程，则进行节点身份认证。

图 6 是表示用于本发明一个实施例的密钥组件的实例的示意图以及用于认证获得的密钥组件之间的信息流的示意图。私有密钥 42 本地存储在节点 10 或 12 并且决不会通过网络发送。无论是全球 ATM10 还是远程操作员接口 12，用于本发明的实施例的网络节点在节点配置时就自动接收其身份认证证书。这一般在节点的初始配置时进行，但是如果需要的话也可以在后续的再次配置时进行。节点 10 或 12 首先产生认证请求 44 和公用/私有密钥对。该公用密钥 46 与认证请求打包在一起，并通过分布组件目标模块（DCOM）发送到 CA14，其中，该认证请求包含识别该节点的信息。

参照图 6，当 CA14 接收认证请求 44 时，它检查要进行确认的节点的策略数据库 48。如果请求认证的节点 10 或 12 处于该策略数据库 48 并且

已被许可以用于认证,则发出数字认证证书 50 并更新策略数据库 48 以反映这个事实。认证证书 50 返回节点 10 或 12, 在这里将其输入 IPSec 配置。在这点上, 完成节点身份认证并且节点 10 或 12 能够建立安全通信。如果节点 10 或 12 不在该策略数据库 48, 或还未被赞同可以用于认证, 5 则指示这种情况的一个错误信号返回节点 10 或 12。节点 10 或 12 不能建立与其他节点的安全通信直到其身份已被认证为止。

进一步参照图 6, 在认证节点 10 或 12 之后, 后续的认证请求导致返回节点 10 或 12 的错误信号, 除非在策略数据库 48 内节点 10 或 12 已被再次赞同可以用于认证。CA14 上的策略数据库 48 可以被周期性地仔细阅读以检验已经认证过的所有节点。如果节点在策略数据库 48 已被许可, 10 但是还没有被认证, 则应该研究这种情况并纠正这种差异。注意到下面的这一点是很重要的, 即, 认证请求 44 和产生的认证 50 被分别打包在不同的格式内并且不能进行任何方式的加密, 或者说, 它们在本质上是不敏感的。请求 44 和认证证书 50 仅包含初步识别信息和节点的公用密钥 46, 15 以及确认认证证书 46 的完整性所必须的信息。节点的私有密钥 42 决不开节点 10 或 12 本身。节点的私有密钥 42 在任何时间都不通过网络 24 发送。

在本发明的一个实施例的这一方面, 隧道操作对于驻留在全球 ATM10 和远程操作员接口 12 或 26 上的应用程序来说完全透明。根据配置时间所 20 建立的设置, 按照要求自动协商并建立安全隧道 30 或 32。隧道的建立不需要完成与 CA14 的交互作用。当安全性关联 (SA) 寿命到期时自动再次协商隧道 30 或 32, 并且当停止节点 10 和 12 之间的网络通信量时, 在 SA 寿命到期时还自动终止隧道 30 或 32。

数字认证证书仅对于有限的时间量有效, 并且在该时间过去之后, 认 25 证证书到期并且不再有用。本发明一个实施例的附加特征包括对节点自动

再次认证证书的支持。

图 7 是表示用于本发明一个实施例的 IPSec 的配置参数的实例以及所选择的如何设定这些参数的实例的表。这样的配置产生一个极为安全的隧道环境。这样的配置基本上是 IPSec 或任何其他替换物可提供的最安全的配置。图 8 是表示用于本发明一个实施例的必须允许的以便能够支持安全通信的端口和协议以及远程操作员接口功能性的实例的表。

在本发明的这一方面，在整个配置中必须相对较早建立 CA14，因为它的根认证证书 40 需要用于后续的全球 ATM 和远程操作员接口节点配置。CA14 是一个驻留在数据中心或其他被保护的环境的专用服务器，并且具有发出检验节点身份的数字认证证书的责任。CA14 包含策略数据库 48，必须管理策略数据库 48 以便许可对特定网络节点（一个或多个）的数字认证证书的发出。根据操作人员之间的职责分工，在接近实际外部系统管理部件 22 处可以设置 CA14，以便同一个操作者可以管理 CA14，或者可以在与外部系统管理部件 22 实际隔开处设置 CA14，以便在新的网络节点许可之前提供一个附加的操作检查点。作为一种替换，可以采用制造者/检查者程序模块以实现相同目的。

在本发明的一个实施例中，CA14 最好是一个专用机，不可用于任何其他目的。适用于 CA14 的硬件包括例如具有 1GB HDD(推荐 4GB)和 64MB RAM 的奔腾级个人计算机(PC)，CD-ROM，具在 SVGA 能力的显示器，以及网络接口卡(NIC)。适用于 CA14 的软件包括例如微软的 Windows NT 4.0 服务器，Network Associates NetShisld NT 4.03a 或更新版本（在 MCA 之后安装），March Security Manager(SCM) 和 March Event Log Manager(ELM)(在 MAC 之后安装)。另外，MCA 版本必须安装在 CA14。这就将安装包括 Certificate Sever, Windows NT Service Pack 5, 和 Internet Explorer 5.0 的 NT Option Pack 4。

在本发明的一个实施例的安装程序中，在安装 Windows NT 4.0 服务器时具有如下选项：单独的“非主域控制器（非-PDC）”配置、只作为安装网络协议的 TCP/IP、具有未指定域的默认工作组会员资格、以及提示 IIS2.0 安装时选择的‘NO’。机器 14 配置有 IP 地址以用于网络连接。

5 根据下面的程序由 CA 机 14 上的一个管理器安装 MCA 软件版本：

1. 1) 在安装该软件之前关闭所有其他的运行应用程序。

1. 2) 将 MCA CD-ROM 插入 CA 机 14 并从根目录运行 ‘install.bat’；

1. 3) 安装自动运行完成。在安装期间机器 14 重新启动两次，并自动注册回以使安装继续。在完成安装之后，机器 14 第三次重新启动，之后

10 不再进入系统。

1. 4) 登录回到机器 14。

1. 5) 运行“用户管理程序”。

1. 6) 将用户帐户“CertTrans”的口令变成一个新的信息安全许可口令，并将“口令不会期满”设置成“真”。

15 1. 7) 退出“用户管理程序”。

1. 8) 配置“传送服务程序”组件。

按照如下过程，将作为认证传送服务的服务器侧组件的传送服务程序安装到 CA 机 14 上：

2. 1) 从“开始”菜单运行程序“dcomcnfg.exe”；

20 2. 2) 从“应用程序”列表中选择“TransServer.TransClass”并点击“属性”；

2. 3) 从“安全”列表中选择“使用用户访问许可”并单击“编辑...”；

2. 4) 将“所有人”组加到具有“允许访问”的访问类别的表中并单击“OK”；

25 2. 5) 还从“安全”列表中选择“使用用户运行许可”并单击“编辑...”；

2.6) 将“所有人”组加到具有“允许运行”类型的访问类别的表中并单击“OK”；

2.7) 从“身份”列表中选择“这个用户”并输入“CertTrans”作为“CertTrans”帐户的用户和口令。这个口令在上述 MCA 版本的安装步骤 5 1.6 中被改变；

2.8) 单击“OK”以关闭“TransServer.TransClass 属性”窗口。从“默认属性”列表中，确认“在此计算机上启动分布式 COM”，并检验“启动 COM 因特网服务”模块。对于“默认认证等级”，选择“无”，而对于“默认个人等级”，选择“无名”；

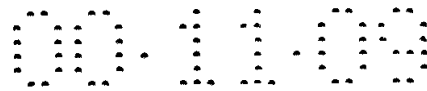
10 2.9) 从“默认协议”列表中，对安装的所有协议选择“删除”。选择“加入”并选择协议“开隧道 (tunneling) TCP/IP”；

2.10) 单击“OK”以完成 DCOM 配置。

为了配置远程过程调用 (RPC)，CIS 需要将服务程序包 4 安装在 Windows NT 服务程序 4.0 计算机 14 上。CIS 还要求包括因特网服务管理 15 程序在内的因特网信息服务程序 4.0 正在运行。IIS4.0 是 Windows NT4.0 的可选程序包。应当注意，CIS 不应被安装在一台运行微软代理服务程序的机器上。RPC 配置过程如下：

3.1) 在“Inetpub”目录下创建一个 RPC 子目录。例如，在命令提示行，键入“md c:\inetpub\rpc”或利用 Explorer 创建该文件夹。这个 20 目录在下面的指令中称之为“%inetpub%\rpc”，而在提示时，键入实际的物理路径，即“c:\inetpub\rpc”；

3.2) 将“Rpcproxy.dll”从 Windows 系统目录复制到“%inetpub%\rpc”。例如，在命令提示行，键入“copy%windir%\system32\rpcproxy.dll c:\inetpub\rpc”或利用 25 Explorer 复制文件；



3.3) 为创建的目录创建一个虚拟根。为此：从“开始”菜单，选择“程序”，指向“Windows NT4.0 可选程序包”，然后指向“微软因特网信息服务程序”，并单击“因特网服务程序管理程序”。在控制树（左侧的窗格）中，选择“控制根/IIS/<机器名>/默认站点”。用右键单击“默认站点”，单击“新生成”，再单击“虚拟目录”。在“新虚拟目录”向导中，为“用于访问虚拟目录的别名”输入“RPC”，为“物理路径”输入“%Inetpub%\rpc”，为“许可”输入“执行访问”；

3.4) 不关闭“因特网服务管理程序”，将对“默认站点”的连接超时设置为“5 分钟”。为此，在控制树中（左侧窗格），选择“控制根/IIS/<机器名>/默认站点”；用右键单击“默认站点”，然后单击“属性”；在“默认站点属性”对话框中，选择“站点”列表；将“连接超时”变为“300”；在不关闭“因特网服务管理程序”的情况下单击“OK”；安装“RPC 代理 ISAPI 滤波器”；在控制树（左侧窗格）中选择“控制根/IIS/<机器名>”；右键单击机器名；单击“属性”；为“主 WWW 服务属性”选择“编辑”；选择“ISAPI 滤波器”列表；选择“加入”；然后为“滤波器名”输入“Rpcproxy”，为“可执行”输入“%Inetput%\rpc\rpcproxy.dll”；

3.5) 然后关闭“因特网服务管理程序”。现在完成了 RPC 和传送服务程序的配置，重新启动机器 14 以使前述变更生效。

由 MCA 版本配置 CA14 以便遵照信息安全策略和标准。商务应当确保将对 CA 机 14 的实际访问限制在遵照信息保密策略，应当安装 Network Associates Netshield v4.03a 或更新版本以提供防病毒保护，并应当安装 March Security Manager 和 March Event Log Manager 软件。CA14 的 DCOM 配置只允许从机器 14 外部生成传送服务程序组件。CA14 上的所有其它 COM 组件被限制在只能在本地生成。

CA 根认证证书 40 在节点配置之前就分配给所有的全球 ATM 和远程操

作员接口节点。应当强调，CA 根认证证书 40 不包含秘密或敏感信息。用于分配这个认证证书的三种不同的方法包括基于软盘、基于网络、和基于仓库。对于全球 ATM 和远程操作员接口节点的有限规模分配来说，通过软盘分配根认证证书 40 是最佳的方法。

- 5 对于基于软盘的分配，数据中心人员将根认证证书 40 置于一个或多个软盘中，并且这些磁盘中的一个被制成在节点配置时间现场安装者可以利用。在节点配置的过程中，全球 ATM10 提示插入这个磁盘，在远程操作员接口节点，例如远程操作 PC12 或 26 上，由“Virtual Private Network Configuration Tool”进行提示。根认证证书软盘的生成涉及将一个格式化的空盘插入 CA 的软盘驱动器，并从“c:\certs”目录中将名为“<CA_SERVER_NAME>_eCITICA.crt”的文件复制到软盘中。例如，如果 CA 服务器名为“CertAuth”，则被复制的文件名为“c:\certs\CertAuth_eCITICA.crt”。

15 依据本发明一个实施例的基于网络的根认证证书分配只有远程操作员接口节点可以得到，如远程操作员接口 PC12 或 26。这就是当一个远程操作员接口节点位于不同于这个全球 ATM10 的实际位置、和/或包含根认证证书 40 的软盘不可利用时所选择的方法。对于大型的全球 ATM 分配来说，基于仓库的根认证证书分配是最佳的方法。在生成主图象之后，CA 根认证证书 40 被安装在主机上。然后复制主机内容以生成用于全球 ATM 现场安装的磁盘。生成用于仓库安装的包含根认证证书 40 的软盘的方式与用于基于软盘分配方法的软盘生成方式相同。

25 在本发明的实施例中，策略数据库 48 是 CA14 希望确认的网络节点列表。当新的全球 ATM 或远程操作员接口节点加入到网络中时，必须更新这个列表。通过一种专用的策略数据库管理工具来执行这个任务。由“开始->程序->CA 数据库维护工具”，运行“CA 数据库维护工具”，并自动打

开策略数据库 48。

图 9 是依据本发明实施例的“CA 数据库维护工具”的简单图形用户接口（GUI）屏幕 52。参照图 9，为了将额外的网络节点加入到策略数据库中，单击“加入一个节点”54，GUI52 提示用户输入 IP 地址。该工具对策略数据库 48 做出的任何修改都要记录。还参照图 9，如果一个节点已经具有了由 CA14 认证过的身份，则检查该记录的“认证过的”字段 56，并且认证的日期在“开始”字段 58 中。如果由于某种原因需要再次认证特定的节点，例如由于该节点的硬盘崩溃，则简单地清空“认证过的”字段 56，这将允许将一个新的认证证书发送给该节点。有人建议利用制造商/检验者变化表格来管理策略数据库 48。

周期性地仔细研究策略数据库 48 以确认所有被认证许可的节点实际上都已认证过。对策略数据库 48 指示的状态与实际的现场条件之间的任何差异都要进行充分的调查以了解产生这种差异的原因，因为这种情况可能是该字段中不正确活动的早期反映。

在本发明的一个实施例的实施方案中，对节点认证事件进行一次手工确认。更具体地，在策略数据库 48 中已经许可认证这些节点但这些节点实际上还没有被认证时，例如在有效分配期间，就需要一天数次地仔细研究策略数据库 45 或事件记录，并在发生一个节点认证事件时，通过独立地接触现场，对该特定节点的安装进行手工认证。通过现用的事件记录监测和报警工具，可以更容易地实现这种手工确认。在本发明的另一个实施例中，主要是对较大的区域，利用现有的信任关系取代了这个过程步骤。

在本发明的一个实施例中，将 CA 机 14 备份并通过标准数据中心备份机构进行还原。这些备份以安全和受控的方式处理。需要周期性地备份策略数据库 48，在将一个新节点加入到策略数据库 48 中时也要进行备份。

备份策略数据库 48 的过程包括运行 Explorer，定位到目录

“C:\winnt\System32\CertLog”，并将文件“policy.mdb”复制到备份介质上。在从备份介质还原策略数据库 48 时，如果将策略数据库 48 备份到一个软盘上，就将该软盘插入到软盘驱动器中，并将文件“policy.mdb”复制到目录“C:\winnt\System32\CertLog”上即可。

5 依据本发明的一个实施例，对远程操作员接口 12 或 26 的硬件要求包括例如一台具有 1GB HDD，32MB RAM，CD-ROM，1024*768*256 显示器和一个网络接口卡（NIC）的奔腾 PC 机。依据本发明的一个实施例，对远程操作员接口 12 或 26 的软件要求包括例如微软的 Windows NT4.0 Workstation, Windows NT 4.0 Service Pack 5 以上，Internet Explorer
10 4.01 以上，和 Network Associates NetShield NT 4.03a 以上。另外，VPN 版本安装在远程操作员接口节点 12 或 26 上。还安装了 IRE SafeNet/Soft-PK v 2.1.0 和 Virtual Private Network Configuration Tool。

安装和配置一个远程操作员接口节点，如远程操作 PC12 或 26，用于
15 与全球 ATM10 进行安全通信，这一过程需要远程操作员接口机 12 或 26 的管理特许，以执行安装和配置。按照如下过程将 VPN 版本安装到远程操作员接口机 12 或 26 上：

4.1) 在安装该软件之前关闭所有正在运行的其它应用程序；

4.2) 将 VPN CD-ROM 插入到机器 12 或 26 中并运行来自根目录的
20 “Setup.exe”；

4.3) 除提示输入用户名和公司名称的注册屏外，接受所有的默认选择；

4.4) 在完成安装之后选择“重新启动”选项。

在机器 12 或 26 重新启动之后，在配置机器 12 或 26 进行安全通信
25 之前，必须安装 CA 根认证证书 40。如果 CA 根认证证书软盘可用，则通

过 Virtual Private Network Configuration Tool 执行根认证证书 40 的安装。如果 CA 根认证证书软盘不可用，则通过网络浏览器获取根认证证书 40。

基于网络获得根认证证书 40 的过程如下：

5 5.1) 打 开 URL ,
 “http://<CA_SERVER_NAME>/CertSrv/CertEnroll/cacerts.htm” 。 例
 如，如果 CA 服务器名为 “CertAuth”，则打开 URL，“http://CertAuth
 /CertSrv/CertEnroll/cacerts.htm” ；

10 5.2) 一旦在用户的浏览器中显示该页，选择 “Certificate for....”
 链接。这是与一个包含 CA 根认证证书 40 的文件的链接。出现一个对话框
 询问用户是想打开该文件还是保存该文件。该文件被存为
 “c:\temp\cert.der” 。

5.3) 从 “开始” 菜单，“运行...” 程序 “cmd.exe” ； 以及

15 5.4) 输 入 命 令 “ cd\winnt\system32” 和 “ scriptit
 CertImport.ini” 。随后的不超过 30 秒的处理过程不被中断。当完成该
 过程时，引入 CA 根认证证书 40 备用。

依据本发明的实施例，Virtual Private Network Configuration Tool 按照如下过程配置远程操作员接口机 12 或 26，以建立与全球 ATM10 的安全通信：

20 6.1) 从 “开始->程序”，运行 “VPN 配置” 并跟随提示；

6.2) 如果在以前的步骤中没有安装 CA 根认证证书 40，则该工具提示插入包含 CA 根认证证书的软盘；

25 6.3) 该工具提示输入 CA14 的 IP 地址并试图获得对远程操作员接口
 机 12 或 26 的身份认证。CA14 必须在网络 24 上可用以完成这个步骤。应
 当注意，输入的 IP 地址必须是发送已安装在节点 12 或 26 上的 CA 根认证

证书 40 的 CA14 的 IP 地址，这是非常重要的。

6.4) 一旦获得了身份认证，该工具显示一个简单的用户接口，允许向远程操作员接口机的 Virtual Private Network 增加和删除目的节点。特定远程操作员接口节点 12 或 26 要管理的任何全球 ATM 如 ATM10 的 IP 地址输入到这个用户接口中。还必须配置该全球 ATM10 以便与远程操作员接口机 12 或 26 进行安全通信。

6.5) 在接收来自用户的确认信息的同时，该工具配置系统以支持与这些目的节点进行的安全通信。该工具不会阻塞一个远程操作员接口节点（如远程操作员接口 PC12 或 26）上的所有其它网络连接。只在全球 ATM10 上才需要这种行为，因为远程操作员接口节点不是专用的。

按照当前的信息安全策略和标准通过商务来配置远程操作员接口机，如远程操作员接口 PC12 或 26。这包括利用 WindowsNT，确保对机器 12 或 26 的适当的实际访问和用户访问，实行对用户帐户的口令限制，配置适当的系统核查和事件登录，以及安装认可的防病毒软件，但不限于上述内容。

在本发明的一个实施例中，VPN、GPI 和 GIF 版本安装在全球 ATM10 上以支持安全的网络通信。VPN 软件作为整个全球 ATM 安装的一部分进行安装。在一个全球 ATM，如 ATM10 的初始配置过程中，配置实用程序提示包含 CA 根认证证书 40 的软盘。认证证书在此时引入到全球 ATM10 中。如果该软盘不可用，仍可对全球 ATM10 进行配置，但它将不具有远程操作员接口功能。当软盘变为可用时，全球 ATM10 重新配置以启动安全通信和远程操作员接口功能。

在成功地引入了 CA 根认证证书 40 之后，全球 ATM 配置实用程序提示输入 CA14 的 IP 地址，以便能够请求身份认证。应当注意输入的 IP 地址必须是发送已被引入到该节点（例如远程操作员接口节点 12 或 26）中的

CA 根认证证书 40 的 CA14 的 IP 地址，这是非常重要的。然后配置实用程序提示输入管理该全球 ATM10 的远程操作员接口节点 12 或 26 的 IP 地址。每个全球 ATM 支持多个远程操作员接口连接。

安全连接被配置到输入的远程操作员接口节点中，并且其它的授权连接，如外部系统管理部件 22 和主机 20，也直接配置。此时其它所有与全球 ATM10 的网络连接被阻塞。一旦完成了全球 ATM 配置，就完成了安全 VPN 的配置，可准备使用。在后面的全球 ATM10 的重新配置过程中，再次进行 VPN 配置以反映出输入的操作参数的任何变化。但是，如果该节点已经具有了身份认证，就不再重复这一步骤。由于全球 ATM10 上的安全配置与 VPN 相关，所以在安装和配置时自动进行全球 ATM10 上的安全配置。

商务有责任遵从有关帐户口令的信息安全策略和限制。但是，在全球 ATM 环境中诸如口令期满和锁定之类的事件的引入在程序上具有重大的冲击。在现有的程序和现场要求范围内能够理解这种冲击。同样地，商务必须实现允许实施这些策略和限制的程序，并且必须能够加强这些策略和限制。操作员接口具有加强与帐户口令相关的信息安全策略和限制的能力。

在本发明的一个实施例中，所有全球 ATM10 操作不需要的端口都是无效的。因特网控制消息协议（ICMP）应答在全球 ATM10 上无效并且不会响应来自另一个网络节点的脉冲信号，除非该节点在配置该全球 ATM10 时已被明确授权。为了进行网络故障诊断，ICMP 实用程序“tracert”出现在全球 ATM10 上。它被配置成只支持用于通信的传输控制协议（TCP）和用户数据报协议（UDP）。简单网络管理协议（SNMP）在全球 ATM10 上完全无效。

在本发明的一个实施例中，考虑到 CA 的不可用性对 VPN 客户的影响，特别考虑到如果 CA14 是不可用的，那么全球 ATM10 和远程操作员接口端

节点 12 或 26 在操作上和在安装/配制时是如何受到影响的。CA 不可用性在操作上只有一个重要的影响。如果 CA14 在一个节点的初始配置时间是不可用的，那么该节点的身份将不会被认证。当一个节点的身份还没有被认证时，就不能建立安全连接。通过确保 CA 可用性和策略数据状态，并
5 对该节点进行简单的重新配置，在这一点上的身份认证照常进行，可以恢复这种情况。

再参照图 6，身份认证描述了一个节点从 CA14 获取该节点的数字认证证书 50 的实际过程。这发生在该节点的初始配置时间，并继续通过网络 24 从节点 10 或 12 向 CA14 传输认证请求 44，CA14 确认该请求并通过
10 网络 24 将产生的认证证书 50 返回节点 10 或 12。这是在初始配置过程中节点与 CA14 之间交互作用的全部内容。如果在一个节点的初始配置过程中，CA14 由于某种原因不可用，例如网络 24 故障或 CA14 主机停机，就不会发生身份认证。通过在事件登录中出现的消息，来自源“VPN 配置”的“不能得到客户认证”，可以检测到这种情况。这种故障阻碍了建立从
15 特定节点 10 或 12 或到特定节点 10 或 12 的安全连接，但不会影响阻塞到节点 10 或 12 的非授权连接的能力。

从这种状况恢复是容易的。一旦 CA14 可用，CA 操作人员确认策略数据库 48 反映出节点 10 或 12 没有被认证的事实，简单地对节点 0 或 12 进行重新配置并照常进行身份认证。一旦在节点的初始配置时间或上述恢
20 复方案中已经进行了身份认证，那么在除后面要详细说明了认证期满时之外的后续配置过程中，节点 10 或 12 与 CA14 之间就没有交互作用了。

在依据本发明的一个实施例的一种实施方案中，不包括“认证撤消列表”（CRL）支持。在这个实施方案中，一旦使用端对端的 ATM 网络安全性，就通过认证登记协议（CEP）来管理 CRL 检索。当端对端的 ATM 安全
25 性适当时，CA14 公布认证撤消列表（CRL）。在 CA14 想要使一个已经发

出的认证证书无效的任何时候，由 CA14 更新这个列表。为了保证信任关系的完整性，VPN 节点周期性地检查这个列表。如果 CA14 不可用来公布这个表，则操作继续进行，直到 CA14 恢复成可用才使认证证书作废。

在一个节点的认证期满时，自动进行身份的重新认证。如果此时 CA14 不可用，则基本上与在发生冲击和恢复时的初始节点配置的情况相同。但是具有一个能够进行重新认证的充分大的时间期限。尝试在当前认证期满之前开始重新认证。CA14 在如此长的时期内不可用的可能性是非常低的。但是，如果出现了这种情况，则恢复过程要与初始配置的过程完全相同。

好的安全性需要周期性地对信任关系进行重新确认。因此，数字认证证书具有一个内定的有效周期。这意味着在一个特定日期和时间之前以及在一个特定的稍后日期和时间之后，对任何请求认证的应用程序来说，数字认证证书是无效和不可用的。当 CA14 发出一个数字认证证书时，认证有效期的开始时间被设置成按 GMT 的发出时间，从 CA 的角度来说即为当前时间。有效期的截止时间被设置成稍后的日期，一般为开始时间之后的几个月或几年。

图 10 是依据本发明一个实施例的使用 GMT 的实例的示意图。参照图 10，认证有效期的开始时间总是被设置成发出的 GMT，在此例中为 2000 年 1 月 25 日，19:00。由于这个有效期的存在，产生了 CA14 已经发出了认证证书 50 的情况，但对发往的目的节点来说，该认证仍无效，这就阻止了该节点马上使用认证证书 50。如果在短时间内涉及该认证的 CA14 和被认证的节点在时间上明显不同步，就会发生这种情况。

图 11 表示了认证证书 50 对被认证的节点 10 或 12 无效的情况。例如，如果 CA14 被设置成 1900GMT，而请求认证的节点 10 或 12 被设置成 1700GMT，发给节点 10 或 12 的认证证书 50 具有 1900GMT 的开始有效期，

并在两个小时内对节点无效。

如果例如将 CA14 设置成 1200PST (2000GMT) 并将请求节点 10 或 12 设置成 1200GMT, 这个问题就会发生一些更细微的变化。发出的认证证书 50 具有 2000GMT 的开始有效期并在 8 小时内对请求节点 10 或 12 无效, 和节点 10 或 12 与 CA14 似乎是偶然地设置成同一时间这一事实无关。这就强调了注意时区设置的重要性。这与具有不同时间设置的图 11 所示的情况相似。反之, 如果例如将 CA14 设置成 1200PST (2000GMT) 而将请求节点 10 或 12 设置成 1500EST (2000GMT), 则认证证书 50 立刻有效。

当 CA14 与被认证的端节点, 如全球 ATM10 具有同样的时间, 但另一个试图与被认证的端节点 10 建立安全通信的节点, 如远程操作员接口 PC12 不具有相同的时间时, 这个问题就会发生另一种情形。图 12 依据本发明的一个实施例表示了该认证对其它节点无效的情况。远程操作员接口节点 12 试图利用全球 ATM10 的认证证书 50, 反之亦然, 从可以确认所说的另一个节点的身份并商定一条安全通信信道。如果设置在远程操作员接口节点 12 上的时间早于全球 ATM10 和 CA14 的时间, 则全球 ATM 的认证证书 50 对远程操作员接口节点无效, 并且不能建立安全话路。

参照图 12, CA14 和全球 ATM10 在时间上同步为 2000 年 1 月 25 日 1900GMT。由 CA14 发给全球 ATM10 的认证证书 50 立刻生效并且可为全球 ATM 利用。但是, 试图与全球 ATM10 建立安全连接的远程操作员接口节点 12 被设置成 2000 年 1 月 25 日 1700GMT。当远程操作员接口节点 12 试图使全球 ATM 的认证证书 50 生效以确认全球 ATM10 的身份时, 由于对远程操作员接口节点来说, 认证证书 50 在两个小时内无效, 所以它不能这么做。而这将阻碍建立安全连接。

由于这些因素, VPN 组织中的所有节点处于相对一致的时基是非常重要的。它们不必同步到秒或分。直到重新启动和也许包括重新启动的节点

配置所需要的实际时间设置延长到足以屏蔽达到几分钟的时间设置差异。

5 由于全球 ATM 端节点已经与主机 20 或外部系统管理部件 22 进行了时间同步，进行合理地时间同步的最重要的输入是 CA14，因为这对于准确确定认证有效期的开始是决定性的。这应当至少与同一主机/外部系统管理部件的时间基本上同步。再者，注意时区和由 GMT 引起的节点偏移的影响是非常重要的。远程操作员接口节点，如远程操作员接口 PC12 或 26 也应当与主机/外部系统管理部件时间大致同步，但这不那么重要，因为这些节点在时间上的任何变化只影响该节点本身，并且只用于反映短时间误差的时间周期。

15 当然这种情况只存在于一个认证寿命的开始。在依据本发明实施例的 VPN 实施方案的一个方面中，在一个认证有效期结尾的认证期满和重新获得是用一种不同方式处理的，并不会碰到这种情况。因此，这种情况很可能只在开发或测试/认证环境中出现，因为实际的现场条件和要求对正确设置时间的规定更为严格。

为实现本发明的各目的，已经对本发明的各个最佳实施例进行了描述。应当认识到这些实施例只是为了说明本发明的原理。各种不偏离本发明的发明构思和保护范围的修改对所属技术领域的技术人员来说是显而易见的。

说明书附图

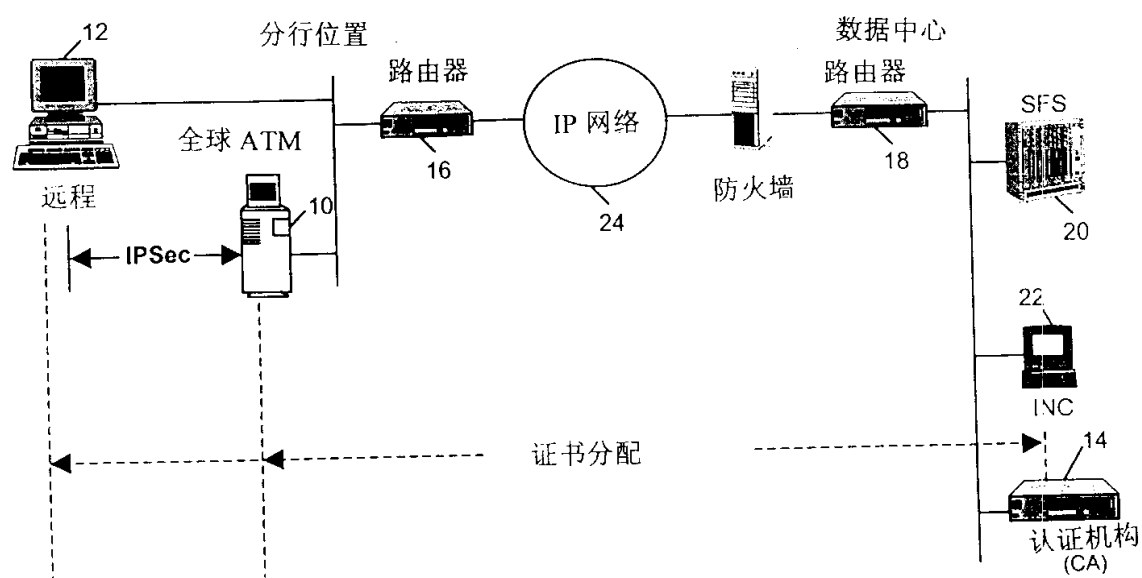


图 1

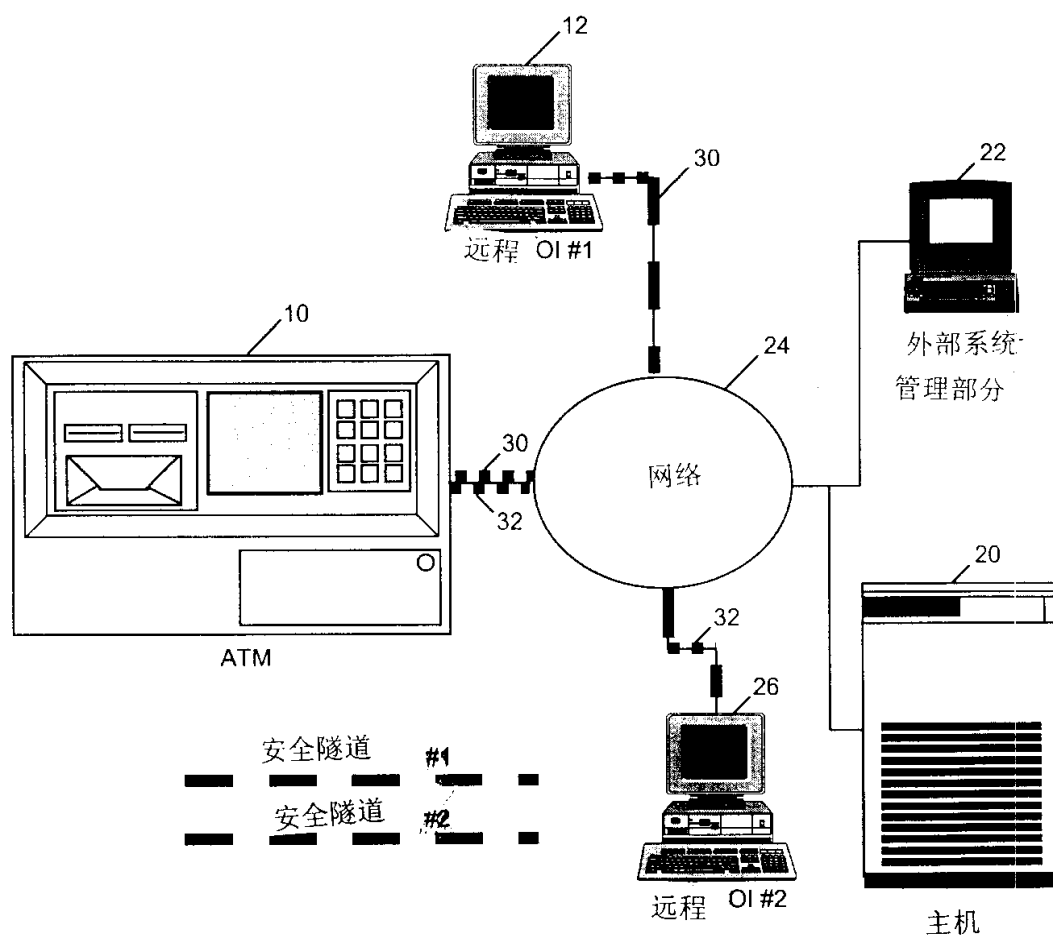


图 2

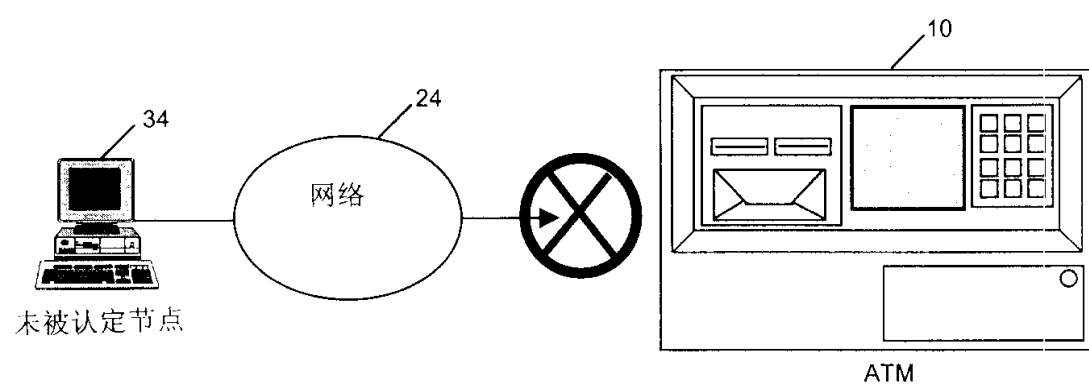


图 3

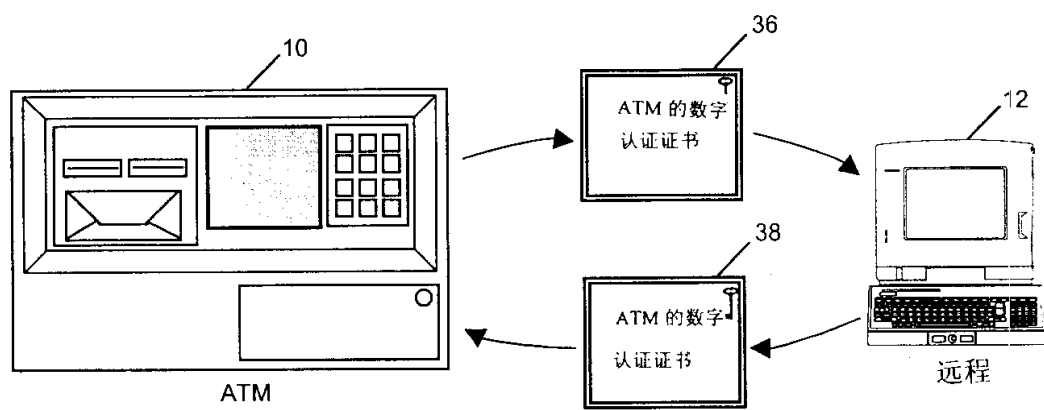


图 4

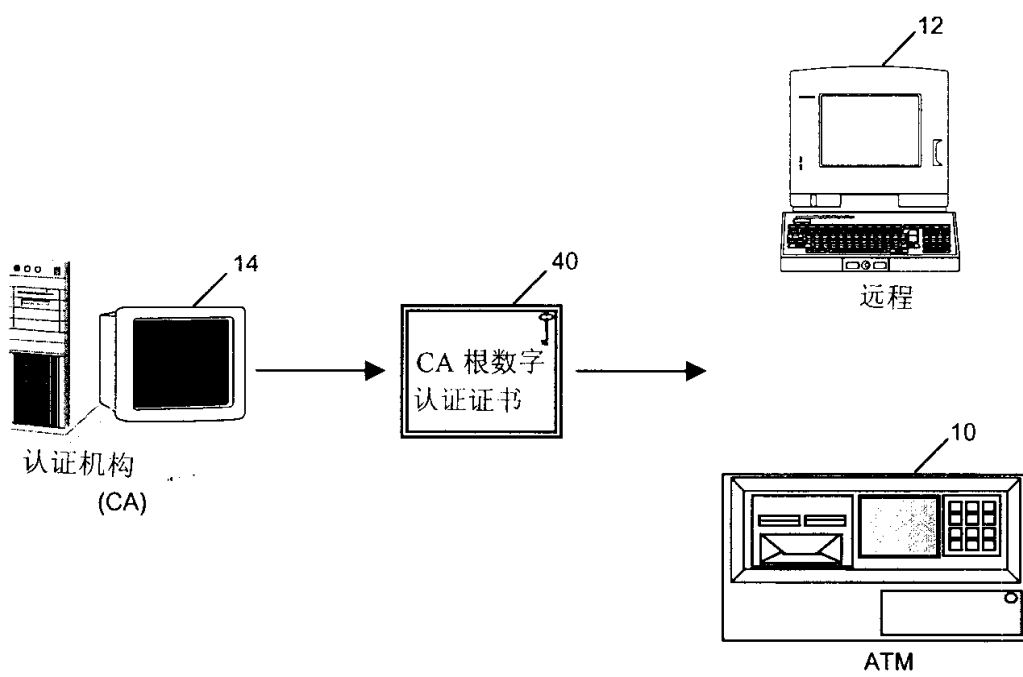


图 5

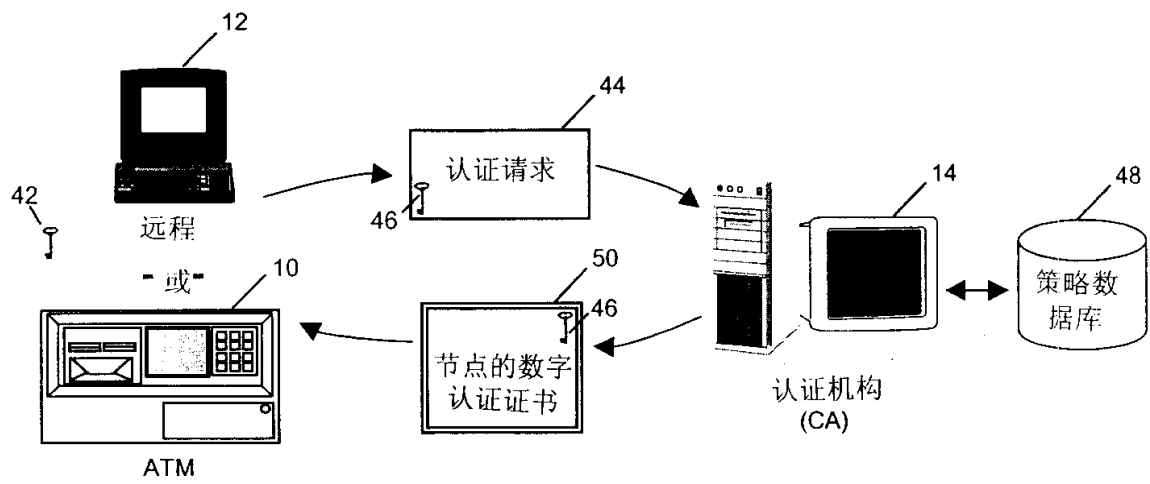


图 6

•	操作模式：隧道
•	认证模式：基于认证证书
•	加密：具有最大长度密钥的 Triple-DES
•	无用信息：HMAC SHA-1
•	完全前向加密：允许
•	重放检测：允许
•	安全性关联（SA）工作寿命：5 分钟

图 7

全球 ATM/远程操作者接口和 CA 之间
- 端口 80 上的 HTTP 和非 HTTP 通信量（DCOM 通过 CIS）
在全球 ATM 和远程操作员接口之间
- 在端口 80 的 HTTP 通信量（浏览通信量）
- 协议 50 和 51（IPSEC 信号交换）
- UDP 端口 500（IKE 密钥交换）

图 8

00.11.09

52

ATM 策略数据库操作程序 1.0

54

增加节点 删除节点 刷新

检索 IP 值 相等 3.0.0.0 找下一个

56 58 在新的一帧中显示所有结果 ☐

	IP	认证过的	开始	期满
	1.1.1.1	No		
	2.2.2.2	No		
	1.0.0.0	No		
	2.0.0.0	No		
▶	3.0.0.0	No		
	4.0.0.0	No		

退出 帮助

图 9

00.11.09

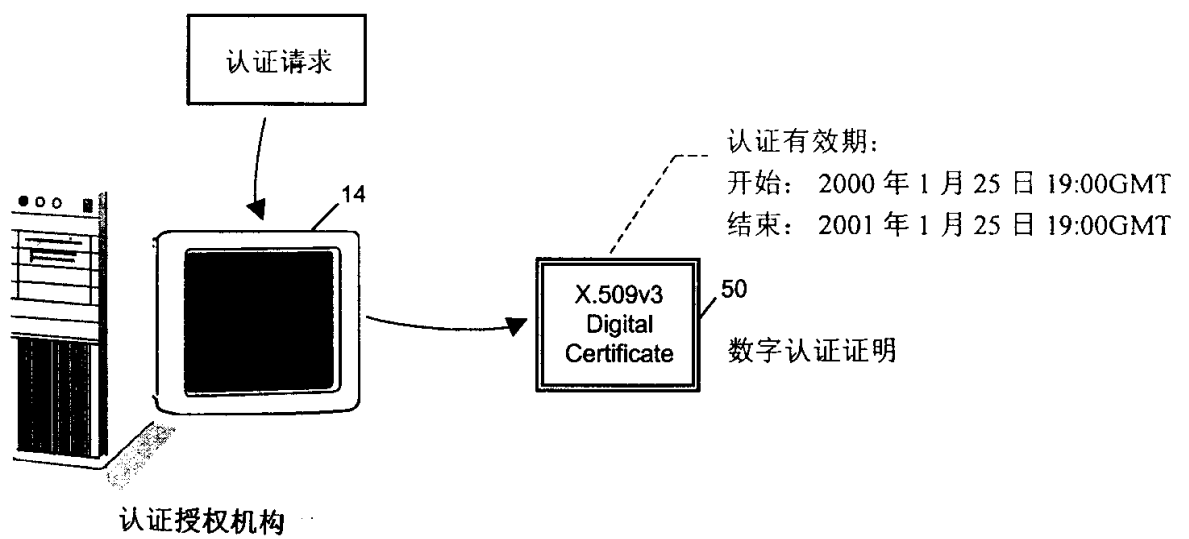
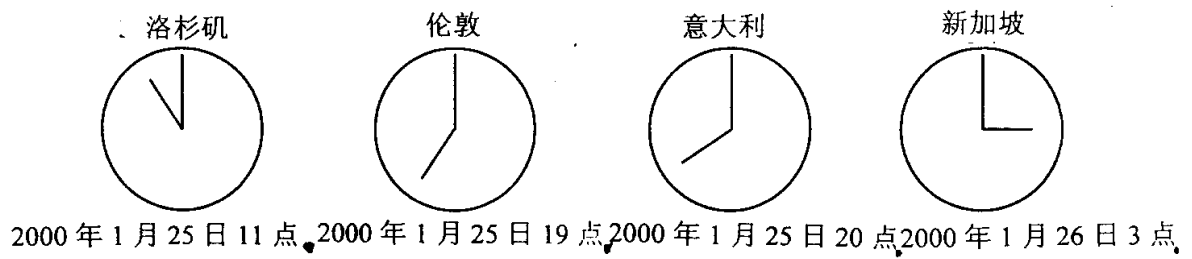


图 10

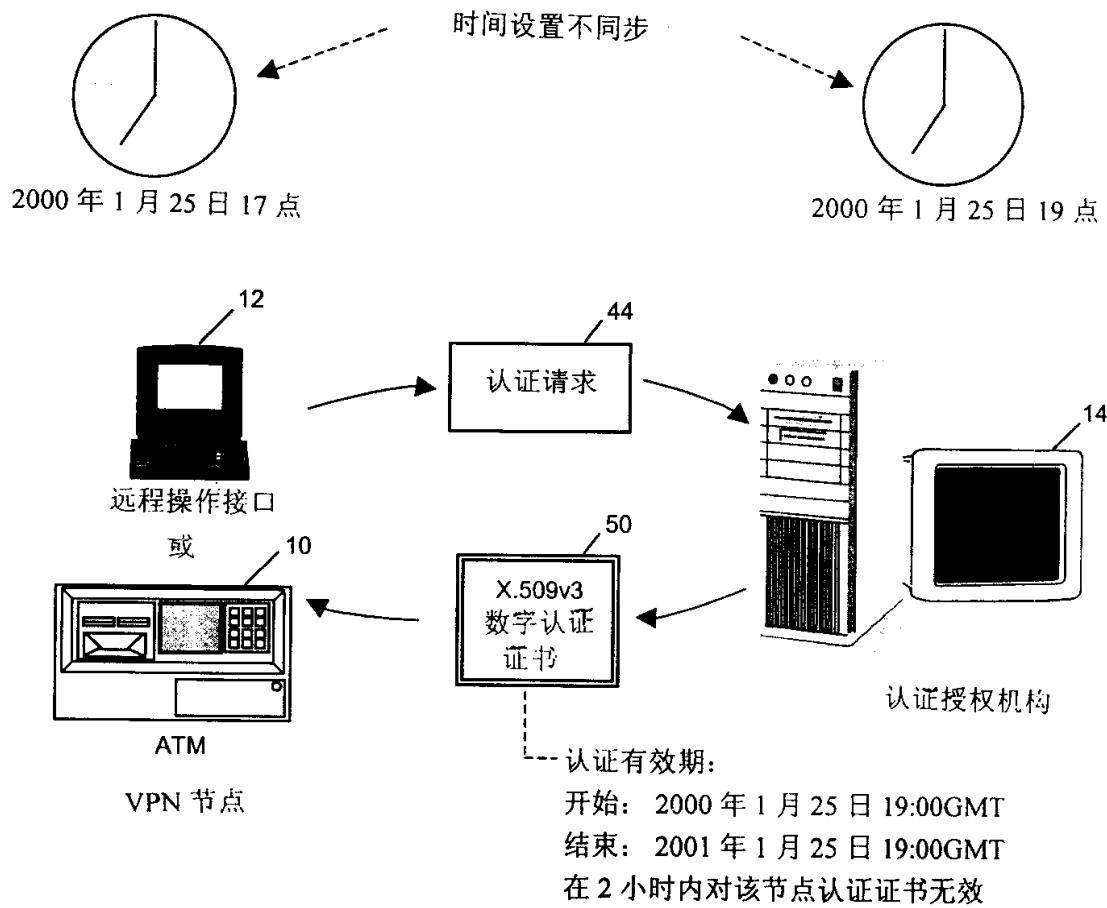


图 11

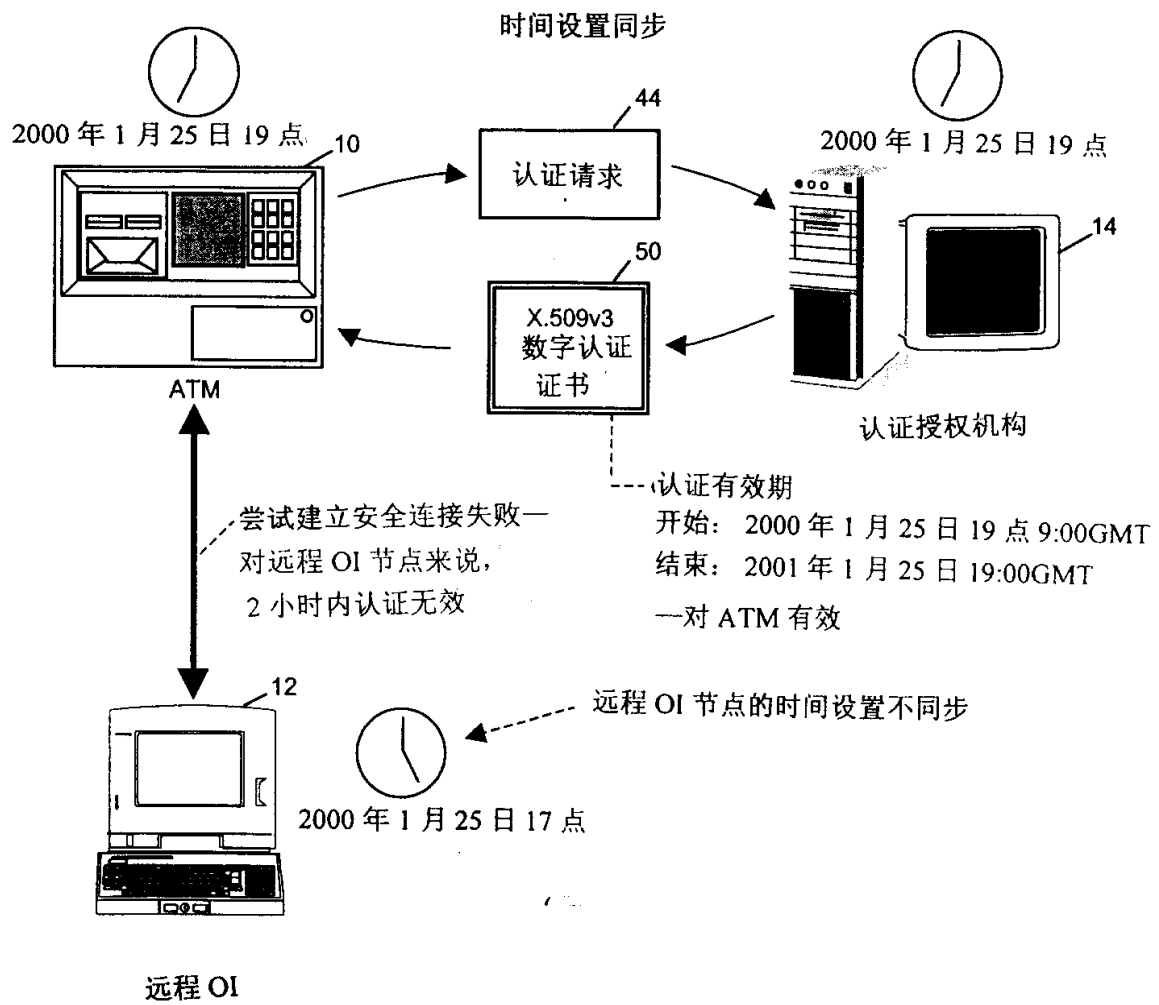


图 12