智能电子商务系统丛书 (3)

# 智能电子商务核心技术内幕

# E-business Digital Certification Guide

# 电子商务数字认证教程

智能电子商务系统丛书编委会 编写


北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

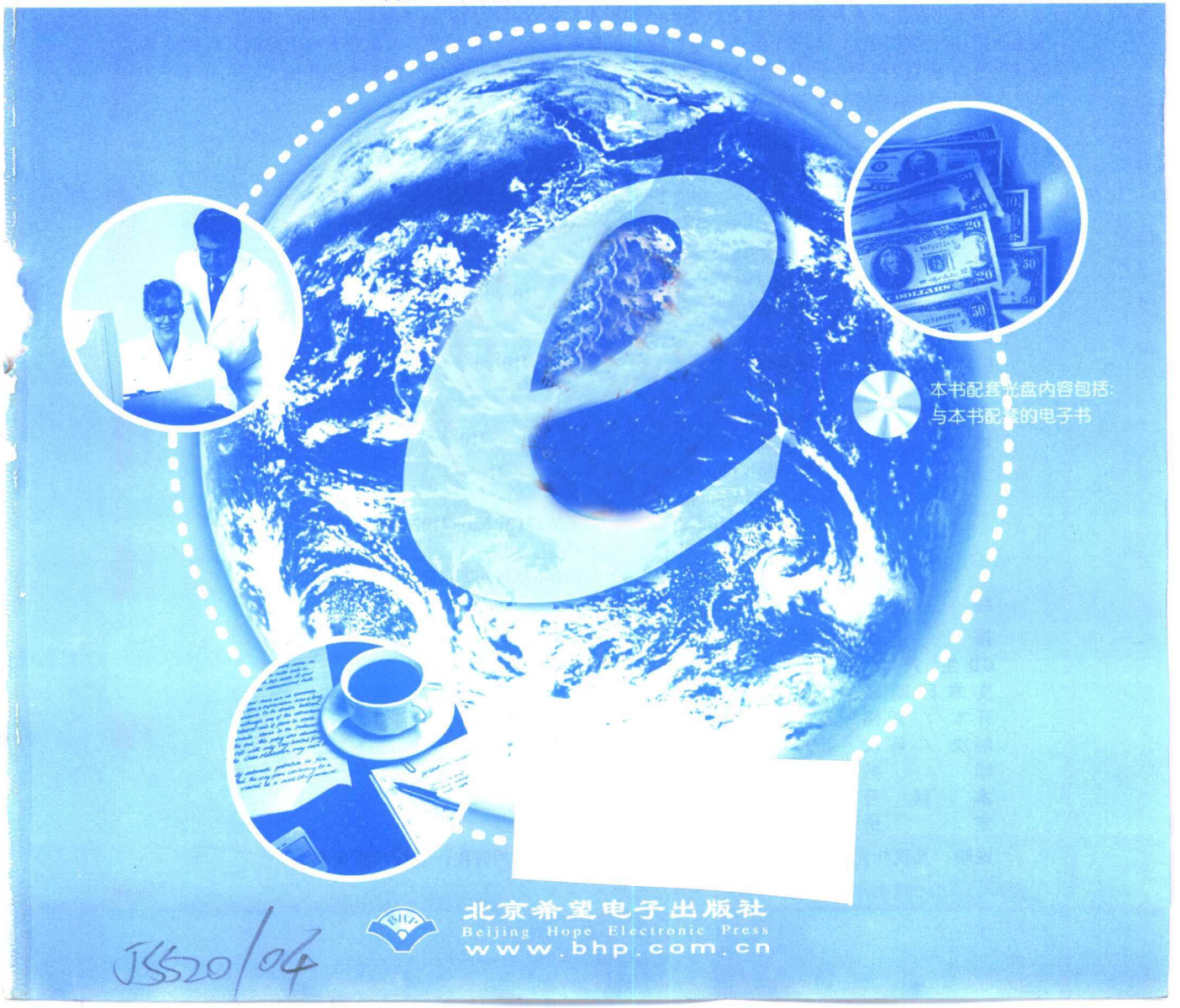
智能电子商务系统丛书 (3)

# 智能电子商务核心技术内幕

# E-business digital Certification Guide

# 电子商务数字认证教程

智能电子商务系统丛书编委会 编写




北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

## 内 容 简 介

IBM 是世界上最大的信息工业跨国公司之一，拥有综合先进技术与结构的全系列产品，包括新一代基于 CMOS 的并行企业服务器、采用 64 位 RISC 技术的 AS/400 高级系列、基于高性能 PowerPC604 微处理器的新 RS/6000 系列以及广泛的软件和网络产品等。在电子商务、复杂的网络管理、系统管理、密集型事务处理、庞大的数据库、强大的可伸缩服务器、系统集成等方面，IBM 具有很强的优势。

目前，IBM 技术和产品已被国内各行各业广泛应用，占有相当的市场份额。为满足技术领域专业人员和用户开发、应用和学习的需要，我社和美国 Austin 技术研究中心以及 IBM 有关专家合作，共同组织出版了本丛书——**21 世纪智能电子商务丛书**（3 本）和 **IBM 核心技术内幕丛书**（7 本）。

本书是“**21 世纪智能电子商务丛书**”一本，是介绍电子商务安全电子手段之一的数字证书的专著。全书共分为三部分，九章。第一部分是全书的概述，包括：数字证书介绍，SSL 概论和数字证书管理器 API 函数介绍，讲述了数字证书的基本概念及有关数字证书的常用术语，这些可以帮助读者更好地理解数字证书；第二部分具体介绍了在 AS/400 系统下使用数字证书的几种方法，包括：AS/400 HTTP 服务器的安全维护，AS / 400 的数字证书管理器 DCM，在 AS/400 标准服务器上启用 SSL；第三部分以具体的用户应用程序范例说明在用户应用程序中使用数字证书的过程，范例 1 为在 ILE RPQ 中使用 API 函数，范例 2 为在 Java 中使用数字证书。

本书重点在于从不同侧面介绍了数字证书的基本知识及其应用，内容新颖、全面，结构合理，具有很强的指导性和实用性，本书不但是从事智能电子商务事务处理系统的广大从业人员重要的开发指导书，而且也是高等院校相关专业师生教学、自学参考书和各科研院所、科技图书馆馆藏图书。

本书配套光盘内容包括与本书配套的电子书。


系　　列　　书：21 世纪智能电子商务丛书（3）
书　　　　名：智能电子商务核心技术内幕：电子商务数字认证教程
文 本 著 作 者：21世纪智能电子商务丛书编委会 编写
责 任 编 辑：苏静
C D 制 作 者：希望多媒体开发中心
C D 测 试 者：希望多媒体测试部
出版、发行者：北京希望电子出版社
地　　　　址：北京海淀路 82 号，100080
网址: www.bhp.com.cn
E-mail: lwm@hope.com.cn
电话: 010-62562329,62541992,62637101,62637102,62633308,62633309
（发行和技术支持）
010-62613322-215（门市）　010-62531267（编辑部）
经　　　　销：各地新华书店、软件连锁店
排　　　　版：希望图书输出中心
CD 生　产　者：北京中新联光盘有限责任公司
文 本 印 刷 者：北京双青印刷厂
开本 / 规格：787 毫米×1092 毫米　1/16 开本　19.5 印张　443 千字
版次 / 印次：2000 年 7 月第 1 版　2000 年 7 月第 1 次印刷
印　　　　数：0001-3000 册
本　版　号：ISBN 7-900044-76-0/TP・76
定　　　　价：50.00 元（1CD，含配套书）

# 智能电子商务系统丛书

## 编 委 会 名 单

# 序

新兴的电子商务，将作为一门学科走进大学殿堂。目前在北京、上海一些有条件的高校已经开设或者正在准备开设电子商务学科。社会相关领域也在举办各种电子商务的培训班。电子商务正在改变我们的社会，正在改变着我们的生活。我国即将加入 WTO，即将成为世界经济贸易大家庭的一员。电子商务正在作为世界经济贸易的一种必须的手段而深受各国政府的高度重视。如何满足社会的需求，培养一大批合格的电子商务人才，是政府部门、企业、高校等正努力的方向。为此我社和美国 Austin 技术研究中心以及 IBM 有关专家合作，共同组织出版了本丛书——**智能电子商务系统丛书**。该丛书由以下 3 种图书组成，主要介绍当前最热门的电子商务技术，包括电子商务事务处理系统开发技术、电子商务技术与数据仓库应用技术和电子商务数字认证系统结构等。下面简要介绍每本书的主要内容。

1.《**电子商务事务处理系统开发教程**》。本书由 3 部分 14 章组成，第一部分“VisualAge Generator Web-Transaction 程序设计”，讨论了 VisualAge Generator Web 事务处理，Web 事务处理系统的实现，Web 事务处理程序设计理论及注意事项，从 TUI 到 Web-Transaction 的转换，HTML 和 UI 记录的定义，Java Server Pages 和 UI 记录的 Interface Bean API；第二部分“Web-Transaction 开发”，介绍了开发 Web 事务处理程序的技巧，VisualAge Generator Templates Web 事务处理，VisualAge for Java WebSphere 测试环境；第三部分“系统实现”，内容包括：运行环境方案的实现，建立 VisualAge Generator Web 事务处理程序的运行环境，安装 WebSphere 应用服务器，Web 事务处理程序的生成，运行 Web 事务处理程序。

本书结构清晰，内容丰富。不但详细地介绍了有关 Web 事务处理程序的理论知识，还详细地介绍了利用 VisualAge Generator 开发 Web 事务处理程序的方法。

2.《**电子商务技术与数据仓库应用教程**》。本书由两大篇目组成，涉及两个独立而又相关的主题：智能电子商务和客户/服务器的智能电子商务转变。在电子商务越来越成为现代商务的重要手段的时代，智能商务将电子商务提高到了一个新的高度，本书第一篇详细介绍了建立智能商务的过程和所需的各项条件，分为五章，第一章“智能商务简介”介绍有关智能商务的知识及有关的术语；第二章“智能商务的实现和数据仓库的概念”介绍智能商务的实现方式和数据仓库部件；第三章“智能商务项目”则详细介绍了成功开发智能商务项目的过程；第四章“BI 数据来源和移动”的重点是数据的来源和移动，包括数据的复制等；第五章“BI 解决方案体系结构”则阐述了可视数据仓库的内容以及它在工业领域的应用。

本书第二篇着重论述了将商务活动从客户/服务器应用转变为电子商务应用时技术人员所面临的设计考虑，可为技术人员开发电子商务解决方案时提供有价值的参考。该篇由三部分、十一章组成，第一部分“概述”包括：电子商务简介，解决方案的结构；第二部分“设计方法”包括：电子商务转换，采集需求，开发体系结构替选方案，选择体系结构替选方案，选择技术，第三部分“研究设计的考虑”包括：搜寻程序经验，电子商务客户端，因特网和应用服务器，访问企业应用程序和数据。通过阅读本书，读者可以了解到电子商务的概念及其解决方案的结构；在什么情况下开始电子商务的转换，建立一个解决方案的进程，解决方案的技术选择；电子商务解决方案过程中的选项，决策和问题。

本书具有内容新颖、权威的特点，书中所涉及的都是当前最有前景的计算机商业技术，以给时代前端的卓有远见的企业技术人员一些指导。本书最重要的特点是不同于一般对电子商务原理讲解的书籍，书中描述了进行电子商务方案开发的宝贵经验和方法，对于想要开发一个电子商务解决方案的设计人员来说，这是至关重要的。本书层次分明，通俗易懂，不仅适用于相关的设计人员，对于想对电子商务有

所了解的人员来说，也能提供有益的帮助。

3.《**电子商务数字认证教程**》。本书介绍电子商务安全电子手段之一的数字证书系统结构。

全书共分为三部分九章。第一部分是全书的概述，包括：数字证书介绍，SSL 概论和数字证书管理器 API 函数介绍，讲述了数字证书的基本概念及有关数字证书的常用术语，可以帮助读者更好地理解数字证书；第二部分具体介绍了在 AS/400 系统下使用数字证书的几种方法，包括：AS/400 HTTP 服务器的安全维护，AS/400 的数字证书管理器 DCM，在 AS/400 标准服务器上启用 SSL；第三部分以具体的用户应用程序范例说明在用户应用程序中使用数字证书的过程，范例 1 为在 ILE RPQ 中使用 API 函数，范例 2 为在 Java 中使用数字证书。

本书重点在于从不同侧面介绍了数字证书的基本概念及其应用，能满足大多数数字证书用户的需求，指导他们在电子商务活动过程中获得最大的利益。本书内容新颖、全面，结构合理，具有很强的指导性和实用性，本书读者可以是计算机专业或非计算机专业对 IBM 公司的 IMS 数据库产品感兴趣的广大用户。

本丛书反映了 90 年代末 21 世纪初国际电子商务技术的最新发展，内容定位与国内外技术和产品市场同步，技术内涵高、内容和范例丰富，实用性和指导性强，特别是针对当前电子商务技术应用与开发人员、技术支持和管理人员，具有很强的参考价值，是以上人员学习和必备的重要技术教程和参考书，同时也是高等院校已经开设或正在开设电子商务学科的首选教学参考书或教材，高校相关专业师生教学、自学参考书和国内各科技图书馆、科研机构重要的馆藏图书。

藉本丛书出版之际，特别感谢美国 Austin 技术研究中心主任戈里高·海登博格教授，IBM 全球支持中心副主任范加尔·茨格博士，本丛书就是在他们的大力帮助和协调下才得以完成。感谢美国 Austin 技术研究中心米歇尔·李博士、IBM 系统开发专家奥列佛·帕登博士、IBM 加拿大公司技术总监屈里奇·托马斯教授、IBM 数据仓库专家莫里哀·琴妮女士，以及 MIT 计算机科学系斯蒂芬·高奇教授和 Tivoli 公司专家汤米·贾维奇先生，由于他们的技术指导和全力参与，本丛书才得以及时完稿。还要感谢马宏华、张中民、李春葆、陆卫民、苏静等，是他们夜以继日的辛勤劳动，使本丛书及时面市。真诚感谢参与本丛书编写的全体专家和技术人员，以及编辑、美工设计人员和录排人员、光盘制作人员等，是他们的加班、加点、忘我的工作，才使本丛书如期付梓出版。

因出版时间紧迫，书中错误在所难免，敬请读者谅解，并请拨冗指正，以期再版时修订。

智能电子商务系统丛书编委会

2000 年 6 月

# 目　录

# 第一部分　概述

# 1　数字证书介绍

在目前及将来的计算机环境中有许多实体是通过复杂的 Web 进行联系的，数字证书的产生在这种环境下有许多作用。

数字证书可以将拥有它的实体从其它许多团体中识别出来。这个识别过程可以自动、可靠地进行，这比目前常用的复杂的用户名及口令要方便可靠得多。

数字证书包括一个公共密钥和私有密钥，由它们可以通过一个不太可靠的网络建立一个可靠的连接，同时也能可靠地识别实体。Secure Socket Layer(SSL)协议和 IPSel 协议过去常建立 Virtual Private Networks（VPN），其它一些可靠的 internet 协议也使用数字证书进行可靠的连接。

本章主要介绍论述数字证书时常用到的一些术语，以及它们是怎么工作的，用在哪里。有关公共密钥基本结构的详细说明请参阅“公共密钥的基本结构”。

## 1.1　术语

一旦深入到 internet 或 intranet 的安全领域，你将遇到许多新的词组和术语，这些将为你理解数字证书打下一个很好的基础。

身份验证：用以证明一个实体的身份。

AS/400 DCM：AS/400 数字证书管理器（DCM），是管理数字证书的应用程序。它具有在 AS/400 上建立、存贮、验证数字证书，将它与用户配置文件及应用程序联系起来的功能。

证书：数字证书的简写。有时也指数字 ID。不过这些词都是一个意思，即一种数字证书的形式。有关数字证书的更多介绍请参阅 1.2 节。

认证中心(CA)：签发数字证书的中心，比如 VeriSion 公司、Thante 公司都是 Internet 的数字认证中心。当所需要的信息传给这些中心，并付了费，通过他们的可靠检验后，就可以由这些中心签发数字证书，也可以在你自己的 AS/400 上建立一个认证中心，给与你联系的实体签发数字证书。在一个较大的团体内，只有由知名的可以信任的 CA 签发的数字证书才有可能被接受。

数字证书使用状态(CPS)：CPS 主要是指 CA 签发的数字证书使用的期限和条件。比如：CA 是怎样验证数字证书申请的。在申请或接受 CA 签发的证书之前一定要仔细地检查一下 CPS。

证书撤销清单（CRL）：CRL 是指失效的及不被接受的数字证书的清单，如果一个 CA 支持 CRL，它应该总是最新的，并且对适当的实体有效。

CRL 包括数字证书的一串数字和撤销日期。

注：AS/400DCM 不支持 CRL。

词句短语：它是一个句子或一个词语，同口令一样可以保护数字证书不被一些非法活动破坏。大部分的 CA 需要这个短语来验证数字证书的撤回、恢复或替代申请。在数字证书的申请中一定要指定这个短语。

数字签字：数字签字可以检查数据在传送中是否被篡改，并证明该实体的身份。建立数字签字时，生成的是 Hash 函数，并且用签字者的私有密钥进行加密。加密了的 Hash 函数是签字者的身份，这种方法常用在数字签字中。

另一个团体可以重复使用这种方法，并用签字者的公共密钥来给原始 Hash 函数解密，然后比较结果，如果一致，这个团体就可以确定它的数据没有更改，这个签字者就是创建该数字证书的实体。

辨别名称（DN）：实体属性及等级名称。如：

- 国家：新西兰
- 州或省份：King country
- 地点或城市：Taihape
- 团体名称：Taihape 大学
- 团体单位：羊毛剪切专业
- 一般名称：Fred Dagg

一个实体的 DN 在签发证书的 CA 中是独一无二的。上述这些属性都由 RFC2459 定义。RFC 即 Request for Comments，可以通过 http://www.rfe-editor.org/.来查询。CA 也可以用其它的属性，但不一定被广泛接受。比如邮政编码在一些旧的浏览器中就不能被接受。

实体：指参与到通信网络的人、组织或机器。

Hash 函数：Hash 函数可以保证信息的完整性。信息的发送要使用 Hash 函数，它是一种数学方法，可以得到信息摘要。信息摘要和原始的信息被发送到接收器，接收器用同样的方法得到信息摘要，然后比较，如果二者一致，证明在传送中信息没有被篡改。理想情况下，原始数据中一个 bit 的码改变，则在信息摘要中将有半个 bit 的码改变。

密钥委托中心：一个持有私有密钥的拷贝，并且只发到合法团体的可靠中心。这个中心常常是政府部门。

中间人：这常常指一个第三团体 X，它拦截并且传送其它两个团体之间的通信。团体 X 可以设置几种攻击网络安全的手段。

公共密钥 / 私有密钥：用于给数据加密，具体而言是用私有密钥对数据加密，只能用公共密钥解密，反之亦然。一般这两个密钥中，一个是公共的，另一个是私有的，可靠的，它们也称为不对称密钥。

智能卡：一种物理设备，特别是一种包括处理机及存贮器的卡，它可以用于保存一个人的私有密钥及提供正确的 PIN 或口令，用这个密钥进行加密和解密。因为密钥始终与智能卡在一起，因此这更增加了系统的可靠性。

知名的 CA：知名可靠的 CA，如 VerSign，美国出版局及 Thante 等，这些 CA 签发的数字证书，如 Netscape 公司的浏览器，都预装了应用程序，从而可以立即在这些中心签发数字证书的服务器之间进行可靠的信息传送。

## 1.2 数字证书的定义

数字证书，即数字 ID，是一种电子识别的个人证书。个人和其它实体如服务器都可以使用数字证书。可以把数字证书比作一本护照。护照上的数字证明是由发放处验证的，一般这种部门是由政府管理的。与护照相似，数字证书是由 CA 签发的。CA 是委托签发数字证书的实体，并且能控制设备防止被骗。一个用户可以有许多个由不同的 CA 签发的数字证书，就象我们可以有许多个人身份一样。你相信个人身份会员卡，但更相信护照；同样，你相信一个由不知名的 CA 签发的数字证书，但更相信一个由知名的 CA 签发的数字证书。数字证书一般有一个标准格式，是 X.509 格式。

数字证书主要由以下组成：

- 一串数字。
- DN 格式下创建的实体名称。
- 证书的公共密钥。
- 证书的有效期限。
- 在 DN 格式下签发证书的 CA 名称。
- 签发该证书的 CA 中心附加的信息，一般用于详细说明证书是怎样使用的。用户名一般是 e-mail 或 TCP/IP 地址，一般用另一个标准扩展名存放。
- 签发该证书的 CA 中心的数字签字，它可以证明数字证书的有效性。

与数字证书的公共密钥相对应的私有密钥一般由证书所属实体持有。有时也可由其它一些可靠的团体如密钥委托中心持有。

- 私有密钥必须保密。可以将密钥与口令一起加密存起来。只有通过有口令的应用程序才能看到密钥。另一种解密办法是使用有个人证书号（PIN）的智能卡。

## 1.3 数字证书的作用

数字证书可以用于身份验证，方便地保证由鲜为人知的网络发来的信息的可靠性，同时建立收到的信息的拥有权及完整性。

*身份验证*

正确识别一个实体。数字证书比其它一些方法，如用户名及口令有更大的优越性。

- 数字证书比用户名及口令有更大的可靠性。因为只有拥有私有密钥及口令才能打开它们。
- 与口令不同的是，私有密钥从来不需要发送，因此它被发现的可能性更小。如果使用智能卡，系统会更可靠，因为它还需要对象的物理特性。
- 使用证书验证实体的过程也很可靠，而用户名和口令必须通过网络且有可能被干扰。
- 数字证书可以将实体从其他许多实体中识别出来，不管这些实体的可信度怎样，因为私有密钥可以保证其可靠性。数字证书省去了用户名和口令的许多麻烦。
- 数字证书不易受中间媒介的破坏。

**注意**：当然数字证书也会被误用。比如，Anita 给 Cotin 存有她的数字证书的浏览器

的口令，Cotin 可以用 Anita 的私有密钥就好象他是 Anita 一样。在该例中真正的拥有者 Anita 必须保护好她使用的私有密钥的口令。

方便性

常常在刚开始连接时，实体的数字证书会自动被确定及身份验证。这个过程常被隐去以便使用户在每天刚开始时只要解开私有密钥或往读出器中插入智能卡就能启动服务器而不用输入用户名及口令。如果他们一天内要与许多不同的服务器连接，就能显出其突出的优越性了。

可靠的数据发送

数字证书以 SSL 为基础，SSL 是一种对 TCP/IP 网络发送的数据加密的方法，SSL 可以在运行 TCP/IP 的大部分服务器上使用，从而保证其它人无法干扰或篡改数据。比如 HTTP，Telnet，LDAP，DDM，APIs，AS/400 工具盒都可以用 SSL。

**注意**：要与 SSL 建立可靠的连接，服务器需要有数字证书。HTTP 服务器常用 SSL，但一般它的客户的浏览器又没有数字证书，但不管怎样，浏览器必须知道相应证书的 CA 中心。

个人虚拟网络(VPN)常用数字证书来进行身份验证。要保证 VPN 的加密数据的保密性和完整性，要在 SSL 的下一层实现，以便不再篡改 HTTP 及 Talnet 之类的应用程序。

建立数据的拥有权及完整性

一个实体可以用私有密钥作为数字签字数据发给其它团体。收到数据及数字签字后，接收者可以以此证实数据来自正确的实体且没被篡改。

许多情况下，数据在被接收之前要进行登记，然后，如果有必要再验证数据的拥有权。

## 1.4　怎样获得一个新的数字证书

目前所有的数字认证中心在处理建立新的数字证书的申请时都有所不同，但基本步骤是一样的。

1. 用户进入 CA 的 web 应用程序选择得到数字证书。
2. 用户必须填表。大多数情况下有：

- 姓名
- e-mail 地址
- 国家，地点或城市，团体，团体单位
- 邮政编码
- 询问短语
- 其它任选的信息，如申请数字证书的客户的出生日期
- 付款信息，当然在签发数字证书时不包括付款信息

不同的 CA 提供给数字认证中心的信息不同。

**注意**：在数字证书的申请中并不总要求邮政编码。有时填上邮政编码，反而给有些浏览器出难题。例如 Netscape Communicator 在其数字证书有邮政编码时会不正常地终止。

Netscape Communicator 4.7 可以解决这个问题。

3. 填完表后，客户必须发出去。此时客户，比如 Netscape Communicator 将申请建立一个私有密钥，这个申请由某一信息指示。

4. 建立了私有密钥后，CA 引导客户怎样得到数字证书。许多情况下，客户会得到一个指示怎样得到数字证书 e-mail。

5. CA 根据数字证书申请的分类，确认有关数据，然后创建数字证书。收到数字证书后立即就可以使用了。

## 1.5 设计数字证书的基本结构

认真设计数字证书的基本结构是非常重要的。在开始申请数字证书及使用之前，必须回答一些基本问题。最重要的问题有：

- 数字证书的作用是什么？
- 谁签发数字证书？
- 怎样申请验证新的数字证书？
- 什么机器可以使用数字证书控制应用程序？
- 怎样管理数字证书，验证及执行变化的申请，怎样处理丢失的，泄密的及不喜欢的数字证书？

### 1.5.1 决定什么时候使用数字证书

这部分叙述数字证书的应用场合。

SSL

HTTP 服务器在使用 SSL 时要用数字证书来进行可靠的连接。

如果你的地址可以公用，你的数字证书最好来自于知名的 CA。如果你创建了一个自己的 CA 并用它来给你自己的服务器签发数字证书，访问你的用户要相信你的话，将收到一串问题询问是否相信你、是否接受你的数字证书。但这将给你的访问者带来麻烦。由知名的 CA 登记的服务器的数字证书可以自动被接受。

如果你的地址只可用在你自己的 intranet 上，你可以用本地的 CA 创建自己的服务器的数字证书，这时你可以把数字证书分配给每个雇员的浏览器或培训雇员在他们自己的浏览器上安装。

*客户身份验证*

你可以使用数字证书来识别客户，这样他们就不必给出用户名和口令了。如果这样就要考虑你的应用程序所用的机器能接受哪一种数字证书。有关这方面的内容参见后面的第 4 章及第 6 章。

*数字签字*

你可以用数字证书来给你建立的文件签字，也可以验证你收到的文件的签字，这时要保证应用程序可以得到签字人的公共密钥。一个能使用户都能得到公共密钥的办法是，出版一个通讯录且能通过 LDAP 得到它。还需要签字和验证签字的规则。目前 AS/400 没有

API 函数能完成这些功能。

### 1.5.2　决定由谁签发数字证书

你可以通过自己的 CA 来签发数字证书，但也只能通过这个 CA 来确认这个数字证书。或者你可以接受一个知名的 CA 签发的证书。当然该证书及有关实体要能通过你的可靠检验。

数字证书的目的是建立一个通用认证中心。对一些小的局部的应用程序签发各种独立的证书，以及强迫人们去接受复杂的证书，都对建立通用证书的目的产生了不好的影响。如果那样，你就会陷入类似于采用复杂的用户 ID 和口令的麻烦之中。

如果每个使用证书的应用程序都能接受它自己的证书清单，或分享共用清单，那么签发自己的证书就没有什么优越性了。

如果一个应用程序要在复杂的系统中运行且其身份验证过程较简单的话，那么签发自己的证书，并且使这个应用程序只接受你自己的证书就是一个简单有效的实现这一可靠环境的办法。但是这种方法不适用于复杂的应用程序和复杂的访问层，这时你应用其它方法来辨别不同的访问层。

你可以在证书中附加一些信息来控制一些访问，特别是你不打算让中心以外的人使用这个证书时。这样你在创建自己的证书时就需要插入这些附加信息来篡改你的 CA。这种情况不适用于授权，因为授权时常发生变化，这时就必须创建一个新证书。

注意，AS/400 DCM 不允许在证书中附加信息。

可见，在你决定是由一个知名的 CA 还是由个人 CA 签发证书时，要考虑许多事情。

总的来说，一个知名的 CA 有利于：

- 在 internet 上要求 SSL 服务。
- 在 intranet 上要求 SSL 服务，并且不用培训用户学习如何在他们的浏览器上使用你的证书。
- 不需要操作自己的 CA。
- 接受用户的 CA。
- 签发很多证书并且不需要验证人们给你的信息。

对于规模较大的团体需要取得很多证书，这样，成本问题将影响他们的决策。在这种情况下就有必要建立自己的 CA 了。还有如下因素证明局部 CA 是有必要的：

- 用自己的 CA 控制签发过程。
- 预先对用户进行识别。
- 对团体很信任。

**注意：** 用 AS/400 DCM 创立客户证书的唯一途径是用户通过浏览器进入 DCM。用户必须使用用户名和口令进入 DCM，然后才能申请证书。用户配置文件事先存在。没有别的办法来代表别的实体创建一个证书，也不能用外部程序或类似的来篡改一个已创建的证书。当证书一经创建，就自动与已给定的用户名相关联。

如果知名的 CA 已经签发证书，就需要同时指出 CPS。CPS 包括了在一个 CA 下操作的各种项目和条件。例如，说明证书的签发、验证及废除。