RSA PRESS

数字签名

解释加密、数字签名、数字证书和公钥基础设施

讨论当前标准以及技术、法律和商业问题

包括供应商技术，详细分析各种解决方案的优缺点

Mohan Atreya 等著 贺军 等译

McGraw Hill Education

清华大学出版社
http://www.tup.tsinghua.edu.cn

数字签名

[美] Mohan Atreya 等著

贺 军 等译

清华大学出版社

Mohan Atreya, Ben jamin Hammond, Stephen Paine, Paul Starrett, Stephen Wu
Digital Signatures
ISBN:0-07-219482-0

书　　名：数字签名
作　　者：Mohan Atreya　等著　贺军　等译
出 版 者：清华大学出版社(北京清华大学学研大厦,邮编：100084)
http://www.tup.tsinghua.edu.cn
http://www.tup.com.cn
责任编辑：冯志强
印 刷 者：清华大学印刷厂
发 行 者：新华书店总店北京发行所
开　　本：787×960　1/16　**印张**：21　**字数**：456 千字
版　　次：2003 年 1 月第 1 版　2003 年 1 月第 1 次印刷
书　　号：ISBN 7-302-06114-9/TP・3653
印　　数：0001～4000
定　　价：40.00 元

作者简介

Mohan Atreya 作为 RSA Security 的技术顾问，负责帮助客户和商业伙伴开发最新的数据安全技术，包括公钥基础设施（PKI）、安全协议和算法。他还向客户提供 RSA 的安全产品的技术和销售支持。负责进行产品培训和为客户提供帮助。

Atreya 最近一直忙于建设新加坡电子传输网络（Network for Electronic Transfer Singapore, NETS），他设计和开发了一个电子支付/借记系统，使客户能够在 Internet 上安全地使用现金卡支付贷款。Atreya 从印度 Pilani 的 BITS（Birla Institute of Technology & Science，Birla 理工学院）获得学士学位。在新加坡国立大学（National University of Singapore）获得工程硕士学位，并从南洋理工大学（Nanyang Technological University）获得了科学硕士（通信和网络系统）学位。

Benjamin Hammond 是 RSA Keon PKI 项目的首席工程师和主要开发人员。他从美国爱荷华州立大学（Iowa State University）获得了计算机科学学士学位，在宾夕法尼亚大学（University of Pennsylvania）获得了计算机科学硕士学位。他具有 10 多年的软件开发实践经验，包括在沃顿商学院（Wharton School of Business）和 NEC 系统实验室（NEC Systems Laboratory）的工作经验。

Stephen Paine 的大部分职业生涯中都从事安全领域的工作。他先是为美国海洋公司（U.S.Marine Corps.）工作。专管数字通信和网络安全。他曾在 SUN Microsystems 公司担任安全设计师，在公司 ERP 财务经济系统中应用密码技术和安全措施。目前，他在 RSA Security 任高级软件工程师。

Paul Starrett 在过去的五年中一直是程序员，他为 NASA Ames 的项目从事程序设计工作，并且在网络协会（Network Associates）中担任技术作家。在过去两年半的时间中，他一直在 RSA Security 中担任软件工程师，从事与 PKI 相关应用程序编写工作。他在美国加州获得了的律师营业执照，喜欢研究信息安全及相关的法律课题。他是美国律师协会的信息安全委员会（Information Security Committee of the American Bar Association）的成员，参与编写该委员会出版的 *PKI*

Assessments Guide 一书。他已经出版了 3 本与安全有关的书，并且拥有自己的私人的调查机构。在过去的 10 年中，他已经为公共机构和私人机构调查了上百个白领犯罪和上百万美元的欺诈案件。

Stephen Wu 是 InfoSec Law Group、PC 和 Infoliance 公司的总裁和 CEO。他是美国律师协会信息安全委员会的联合主席，该委员会在 1996 年出版了 *Digital Signature Guidelines*，在 2001 年出版了 *PKI Assessment Guidelines*。他经常做有关数字签名、数字证书和 PKI 的演讲。他与人合作编写了 *Internet X.509 Public Key Infrastructure Certificate Policy and Certifcation Practices Framework*，即 RFC 2527。Wu 于 1988 年从哈佛法学院（Harvard Law School）毕业，在创建 InfoSec Law Group 和 Infoliance 之前，他负责制订了 VeriSign 公司世界范围的策略并管理其认证服务。在加入 VeriSign 公司之前，Wu 在两家法律公司中从事计算机法律、知识产权和诉讼领域的工作。

前言

欢迎您购买本书。本书是 RSA Press 有关安全方面的最新书目，由 5 位在开发和应用数字签名方面的资深专家编写（其中的 4 位曾在 RSA Security 工作过）。在现今有关数字签名的书中，本书是最全面且最有深度的，其中的各个章节并非仅仅针对技术问题，还从商业和法律的角度充分考虑。本书将会成为您工作的利器。

在最近的几年中，数字密码术已经有了长足的发展。事实上，人们一致认为，如果没有这项技术，就不可能有全球化的电子商务和公司基础设施安全可靠的运转。数字签名就像手写签名一样，可以保证邮件发送者或合同签署者的身份确实无误。在网络和在线销售商确定用户身份时，看到用户签署的名字与看到一个活生生的人是安全不同的。

利用数字签名，公司可以在线联系、购买和销售产品，并在桌面服务器上收集和存储在法律上有效的交易记录。客户将会享受到保障重要电子服务的安全所带来的方便，从购买保险、获得抵押贷款，到可以随时使用佣金账户，而无需等待来回邮寄书面文档。数字签名与手写签名具有相同的法律效力，可以实现 4 个安全目的：机密性、认证、完整性和非否认性。

然而，现在这项技术仍处于发展阶段，仍然存在着大量需要解决的问题。美国、联合国和世界上的许多国家已经制订了不同的法律条款，有些处于实际应用阶段，而有些尚待实施，还需要进行各方面的协调，才能在全世界的范围内实现数字签名。在与安全相关的活动中，隐私权的问题至关重要，对于数字签名来说也是如此，因为要用它来代替实际的、可见的、具有法律约束力的人的“存在”。其他尚需解决的问题还有：各种签名之间的不同（多人签名、证实者的签名、代理签名以及团体签名）；数字签名如何与证据法一致；在法庭上，书面签名、数字签名和签字签名是否具有同等的法律效力。

本书提出了尚有争议的各个问题，使读者能够理解数字签名现在的状况，以及如何在将来最充分地利用它。本书的附录介绍了将影响数字签名应用和实施的主要法规。

RSA Security 的工作重点是安全和认证。在短短的几年时间中，我们亲眼目睹了此行业技术上令人难以置信的飞速发展。在安全领域，数字签名实际上是“即将应用的首要大事”。现在，我们应当清楚这一点，并准备更广泛地应用它。本书可以作为这方面的指南，提供背景知识，深入说明事物的性质，并为各类读者指明方向，其价值无法衡量。本书适用于实现和管理数字签名技术的读者，以及在现实世界中利用和保护数字签名技术的读者。

希望本书能够像 RSA Press 以前出版的得到读者高度好评的其他一样，为读者带来知识和力量。希望您将自己的意见和建议反馈给我们，有关 RSA Security 的更多信息，请访问网站：www.rsasecurity.com。要更多地了解 RSA Press，请访问 www.rsapress.com。

Arthur Coviello
董事长，CEO
RSA Security 公司

目录

第1章

概　述

本章将讨论以下主题：

- 文件无处不在
- 术语
- 技术
- 可用性
- 立法
- 动机
- 综述

你是否常去医院就诊呢？就诊时并不总是在两三个科室进行吧？仅仅是一次例行的身体检查，却要到 3 个不同的科室，这种情况并不少见。当你从一个科室走到另外一个科室时，是否想知道自己的病历到底在什么地方？也许你当时就带着它，也许助理医生帮你带着。无论是哪种情形，如果病历丢失、被盗，或者其他人更改了你的个人医疗信息，将会发生什么事情呢？

1.1 文件无处不在

在当今的数字化世界中，每天创建和保存的电子文档数量正在以惊人的速度增加着。公共用户和私人用户都同样感受到了电子商务系统所带来的好处。

我们再来看一下刚才的医疗事例。美国政府统计局估计，每年 3 千 4 百万的住院量和 12 亿人次的看病数量，会产生大约 100 亿页的医疗病历。此外，医疗数据不仅非常庞大，而且其组织管理也相当混乱。有时，以书面形式保留的医疗记录和文档在需要时往往找不到。另一方面，为了易于查找，同一个书面文件可能会有多个副本，但如何能保证所有这些副本都是最新的呢？

在这种情形中，人们可以很快看到使用电子文档的好处。电子文档信息结构成本低，质量高，在经济和社会生活的所有方面都提供了难以言表的好处。随着这种转化的加速，人们越来越多地提出要求，希望律师就创建、接收、传输、破坏以及把书面文件转化为电子记录等方面的法律后果提出建议。与数字系统和服务相关的数字签名、网络安全以及合同与许可证，都会在现代法律的实施中起到关键的作用。医疗领域特别注重机密性，就像严格的生存和死亡时间依赖于信息的正确性和时间性一样，这些对不断涌现的信息技术提出了最强劲的挑战，同时也带来了最大的机会。这种转变是否成功，法律和政策基础设施所支持的计算机网络至关重要。