

Windows 2000 安全技术

[美] Roberta Bragg 著
倪晓强 沈立 译
杨洪涛 审校

- 理解核心安全概念, 例如密码学、安全协议、PKI 和 Kerberos
- 利用 Kerberos、加密文件系统、NTFS、本地安全策略和 Windows 2000 专用的安全工具控制对 Windows 2000 系统的访问
- 通过 RAS、VPN、PPTP 和终端服务建立安全的远程访问
- 使用记账策略、IPSec、PKI 和组策略等分布式安全服务保护网络的安全
- 实现安全的安装和升级、维护和管理你的安全策略
- 配置访问策略、受限组成员以及系统服务安全
- 保护局域网、IISDA 连接、终端服务和互操作服务的安全



清华大学出版社

<http://www.tup.tsinghua.edu.cn>

NRP

北京科海培训中心

Windows 2000 安全技术

[美] Roberta Bragg 著

倪晓强 沈立 译

杨洪涛 审校

清华大学出版社

(京)新登字 158 号

北京市版权局著作权合同登记号: 01-2000-2751

内 容 提 要

本书从实用的角度出发,全面地介绍了关于 Windows 2000 的信息系统安全,介绍了大量有关 Windows 2000 安全的工具、特性及结构方面的信息。

全书分四部分,分别介绍了安全的基本概念与定义、操作系统安全的保护、本地网络安全的保护以及实际网络安全的保护。内容包括:密码学简介、相关的安全协议、公钥体系及其建立过程、Kerberos、加密文件系统、NTFS、安全策略及安全工具;此外,还介绍了 Windows 2000 域的安全管理与保护、低级 Windows 客户的保护、新的分布式文件系统;最后,还深入探究了使用 RADIUS 和 RRAS 来保护远程访问、Web 安全以及互操作性方面的内容。

本书通过案例分析进行讲解,文笔流畅,通俗易懂。适合管理和支持 Windows 2000 的网络管理员、欲将网络升级到 Windows 2000 的管理人员、系统安全及审计方面的专业人员学习使用。学习本书不要求具有 Windows NT 及其安全或密码学方面的知识,但需具备基本的网络知识。

Windows 2000 Security

Copyright © 2001 by New Riders Publishing

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher.

本书中文简体字版由美国 New Riders Publishing 公司授权清华大学出版社和北京科海培训中心出版。未经出版者书面允许不得以任何方式复制或抄袭本书内容。

版权所有,盗版必究。

本书封面贴有清华大学出版社激光防伪标签,无标签者不得销售。

书 名: Windows 2000 安全技术

作 者: Roberta Bragg

译 者: 倪晓强 沈立

出版者: 清华大学出版社(北京清华大学校内,邮编 100084)

印刷者: 北京门头沟胶印厂

发行者: 新华书店总店北京科技发行所

开 本: 787×1092 1/16 印张: 26.125 字数: 635 千字

版 次: 2002 年 1 月第 1 版 2002 年 1 月第 1 次印刷

印 数: 0001~5000

书 号: ISBN 7-302-05085-6/TP·2974

定 价: 43.00 元

关于作者

Roberta Bragg 自 1985 年起就使用一台便携式计算机经营着她的咨询公司——Have Computer Will Travel 公司。另外，她还当过销售员、系统管理员、开发人员、专栏评论员、大学教师、商业学校教师以及技术培训师。她当前获得的证书包括 MCSE (Windows NT 3.5.1、4.0 与 Windows 2000)、MCT、MCP+Internet 和 CTT，曾涉足 Mainframe moonlanding, 80 column cards 与 Fortran 等领域。读者可以在 www.mcpmag.com 发现她是一名专栏评论员，可以在 www.spu.edu 上发现她是一位教师，可以在 www.peaceweaver.com 上发现她是一名安全福音传道者。

关于技术评论家

下列这些评论家为《Windows 2000 安全技术》的整个发展过程贡献了他们相当多的专家意见。在此书写作期间，这些热心的专家们对书中技术内容、组织方式及写作方式进行评阅。他们的反馈意见对保证《Windows 2000 安全技术》满足读者对最高质量的技术信息的需求是非常关键的。

David Shackelford 是 ChoicePoint 公司的子公司 IRSC 的网络与计算机业务主管。他的经历包括：当过一名养蜂人，为一家通俗诗杂志筛选来稿，并在 Hewlett-Packard 与 Intel 公司教授过网络课程。他已经作为一名教员、系统工程师、网络设计人员及安全管理员在计算机界工作了十年。David 拥有英语硕士学历，是一名微软认证的系统工程师及培训师，是 New Riders 出版的《Windows 2000 Essential Reference》一书的作者之一，也是 New Rider 出版的《Inside Windows 2000 Server》的一名技术编辑。

Mich Kabay 在 15 岁时就开始学习汇编程序，在 1966 年就在 McGill 大学学习 FORTRAN IV G。在 1976 年，他从 Dartmouth 大学获得了应用统计与无脊椎动物学的博士学位。在 1979 年，他加入了美国一个编译器组，研究一种新的 4GL 与 RDBMS，并负责开发统计句法、编写语法分析器、错误捕捉以及命令语言中的统计功能的代码生成。Kabay 博士于 1980 年加入 Hewlett-Packard 并成为了一名性能专家，赢得了 1982 年的系统工程师年度奖。他曾为《Computer World》、《Network World》、《Computing Canada》、《Secure Computing Magazine》、《NCSA News》、《Information Security Magazine》及几种其他的商业杂志撰写过专栏。他在 1997 年获得了认证系统安全专家（Certified Systems Security Professional, CISSP）的证书。Kabay 博士已发表了 220 多篇关于业务管理与安全的论文，并完成了一本大学教材《The NCSA Guide To Enterprise Security: Protecting Information Assets》（ISBN0-07-033147-2），该教材由 McGraw-Hill 于 1996 年 4 月出版。他是 ICSA 实验室从 1991 年到 1999 年（以前的 NCSA，然后是 ICSA）的教育主管。在 2000 年 1 月，他加入了 Atomtic Tangerine 公司的 INFOSEC 组，担任安全领导。

Brendan McTague 是 Perot Systems 公司的 Gloabal Financial Service 部门的高级系统工程师。他目前为一家主要的欧洲银行的投资银行分部管理一个跨平台的 Internet 工程组。Brendan 从 Temple 大学毕业并获得计算机科学学士学位。他已经在 Windows NT 到 Windows 2000 上工作了超过 5 年，并在 1995 年早期获得了 MCSE 证书。当他不工作时，Brendan 喜欢与他的妻子及儿子在芝加哥郊外的家中度过。欢迎给他提意见，他的电子邮件地址是 brendan.mctague@mindspring.com。

前 言

信息系统安全已经成为每个人都必须关心的话题。只知道口令的用法及文件权限设置已经远远不能满足需要了。如果用户管理、设计、实现、安装或者使用计算机系统，则他有权利、也有义务尽可能保护计算机系统的安全（包括在系统中存储和移动的信息）。

Windows 2000 的设计十分注重安全。存在很多新的特性，对老版本的许多功能也做了增强。如果这些特性被恰当和正确地实现，则它们就能够保护系统与数据。然而，只知道这些特性及如何使用它们还不够：网络管理员必须知道使用它们的理由和场合。最后，网络管理员必须以人们能够理解与维护的方式来实现系统安全。

本书提供了关于 Windows 2000 安全的各个方面的内容，但我们并未打算使它成为一本包罗万象的 Windows 2000 指南，而只是集中讨论了可用来保护 Windows 2000 网络安全的一些服务与工具。

本书的读者

Windows 2000 网络的管理员，或者希望向 Windows 2000 迁移的网络管理人员都可以从本书中找到关于 Windows 2000 安全的安全工具、特性以及构架方面的可靠信息。Windows NT 4.0 爱好者也能从中找到相关的知识。

另外，本书假定读者有一定的网络知识，因此只在活动目录的体系结构方面提供了一些介绍性的内容。需要更多知识的读者可在很多资源（包括附录中列出的）中查找。因此，本书一开始就为那些不了解密码学知识的人提供了一些介绍性的材料。

信息系统安全和审计方面的专业人士会从中找到 Windows 2000 安全所提供的全部细节。如果读者对这个领域并不陌生，则可以跳过关于密码学的介绍性材料。Windows 2000 安全的具体内容在后面的几章中有详细的介绍。

本书的组织结构

本书分成如下的四个部分。

第 1 部分 概念与定义

本部分包括安全的基本概念、密码学、安全相关协议、公钥体系及 Kerberos 等几章。如果读者对这些主题有深入的了解，建议直接跳过，这几章之后提供了 Windows 2000 特有的内容。在与 Windows NT 管理员和 Windows 体系支持者的很多谈话中，我发现他们中有很多人对此问题并没有什么背景知识，但他们还必须处理 Kerberos 或 PKI，或选择加密算法，这就是本书为什么包括介绍性内容的原因。后面的几章将讨论 Windows 2000 如何实

现一个标准，以及如何提供选择，这部分比较冗长，任何已掌握这些概念的读者都可以直接跳到第 2 部分。如果碰到了不熟悉的术语或概念，再回来看看就行了。

第 2 部分 保护操作系统的安全

任何安全程序的第一步都应该是保护基本操作系统的安全。这一部分研究了 Windows 2000 所有版本的公共特征，并涉及了独立系统的安全问题。这一部分主要涵盖 Windows 2000 中的 Kerberos 认证、加密文件系统、NTFS、本地计算机安全策略和 Windows 2000 自带的安全工具方面的内容。

第 3 部分 保护 Microsoft 局域网的安全

现今已很少有未上网的计算机了。计算机的连接范围很广，在世界范围内，网络将家庭用户、企业用户和网络服务提供商连接起来。连接的方式也很多，从拨号连接、局域网连接到包含多种操作系统的广域网连接等等都是其中的一种方式而已。这一部分专门介绍 Windows 局域网，涉及 Windows 2000 域安全管理与保护的内容。另外，还有关于保护低级 Windows 客户及新的分布式文件系统的内容。

第 4 部分 保护现实世界网络的安全

网络大多由多种操作系统组成并涉及大量的计算机。这一部分探究 Windows 2000 保护现实网络安全的特性，从中可以找到关于使用 RADIUS 和 RRAS 来保护远程访问、建立公钥体系、Web 安全以及互操作性方面的内容。

目 录

第1部分 概念与定义

第 1 章 安全的基本概念.....	1
1.1 安全的三个“A”.....	1
1.1.1 认证.....	2
1.1.2 授权.....	4
1.1.3 审核.....	5
1.2 安全策略.....	5
1.3 计算机安全的目标.....	6
1.3.1 完整性.....	6
1.3.2 控制.....	8
1.3.3 可用性.....	8
1.4 其他安全术语.....	9
1.5 更多的信息.....	10
1.6 小结.....	10
第 2 章 密码学介绍.....	11
2.1 历史背景.....	11
2.2 现代的加密算法.....	13
2.2.1 对称密钥密码系统.....	13
2.2.2 非对称密钥密码系统.....	14
2.2.3 公钥体系.....	16
2.2.4 数字签名.....	16
2.2.5 数字编码.....	16
2.3 常用加密算法.....	19
2.3.1 DES.....	19
2.3.2 已被提议用来替代 DES 的算法.....	20
2.3.3 Ron Rivest 算法.....	21
2.3.4 CAST-128.....	21
2.3.5 Diffie-Hellman.....	21
2.3.6 RSA.....	21
2.3.7 散列函数.....	22
2.3.8 将来的希望: 椭圆曲线密码系统.....	23
2.4 攻击方法.....	23

2.5 更多的信息	24
2.6 小结	24
第 3 章 新的协议、产品及 API	25
3.1 与 Web 相关的协议	26
3.1.1 安全套接字层和 HTTPS	26
3.1.2 传输层安全协议 (RFC 2246)	27
3.2 远程访问协议	28
3.2.1 串行线路 Internet 协议 (RFC 1055)	29
3.2.2 点到点协议 (RFC 1661)	29
3.2.3 口令认证协议	29
3.2.4 质询-握手认证协议 (RFC 1994)	29
3.2.5 Microsoft-CHAP 版本 1 (RFC 2433) 和版本 2 (RFC 2759)	30
3.2.6 点到点隧道协议 (RFC 2637)	31
3.2.7 Microsoft 点到点加密机制 (MPPE)	35
3.2.8 第二层隧道协议 (RFC 2661)	35
3.3 IPsec	38
3.3.1 密钥管理	38
3.3.2 安全策略数据库	39
3.3.3 IP 栈实现	40
3.3.4 通信安全协议: AH 与 ESP	40
3.3.5 SA 束	43
3.3.6 性能问题	44
3.4 DHCP 与动态 DNS 之间的安全通信 (RFC 2535, 2136, 2137)	44
3.4.1 公钥 / 私钥的实现 (RFC 2535)	45
3.4.2 通过 Kerberos 5 的 DHCP 认证和使用 DHCP 的 DNS 安全更新	45
3.5 Microsoft 独有的 API 和安全协议	46
3.5.1 服务器控制的加密系统	47
3.5.2 CryptoAPI	47
3.5.3 认证码	48
3.5.4 安全支持提供者接口 (SSPI)	48
3.5.5 LM、NTLM、NTLMv2	48
3.6 更多的信息	50
3.7 小结	50
第 4 章 公钥体系 (PKI)	51
4.1 证书颁发机构	52
4.2 注册颁发机构	52
4.3 证书与密钥	53

4.3.1 X.509 证书	53
4.3.2 简单公钥体系	54
4.3.3 PGP	54
4.3.4 证书验证	54
4.4 证书仓库	55
4.5 证书吊销列表	55
4.5.1 吊销列表的选项	56
4.6 证书信任模型	57
4.6.1 层次型信任模型	58
4.6.2 分布式信任	59
4.6.3 Web 信任	59
4.6.4 用户信任	61
4.6.5 交叉证明	62
4.7 客户与客户软件	62
4.8 PKI 过程	63
4.8.1 时间问题	63
4.8.2 密钥 / 证书生存周期	63
4.8.3 产生	64
4.9 更多的信息	66
4.10 小结	66
第 5 章 Kerberos 基础	67
5.1 Kerberos 基础	68
5.1.1 登录认证: 认证服务交换	69
5.1.2 获得一个票证: 票证授予服务交换	69
5.1.3 访问资源: 客户 / 服务器认证交换	70
5.2 Kerberos 组成和算法	70
5.2.1 组件	70
5.2.2 Kerberos 算法	72
5.3 Kerberos 信任路径	86
5.4 加密和校验和	88
5.5 更多的信息	89
5.6 小结	90

第2部分 保护操作系统的安全

第6章 从头开始考虑安全	91
6.1 用户和组	92
6.1.1 独立系统上的用户和组	92
6.1.2 隐式的用户权限	95
6.2 活动目录介绍	95
6.2.1 活动目录结构	95
6.2.2 域模式	96
6.2.3 组作用域	97
6.2.4 域中默认的组	98
6.2.5 隐式组或系统组	100
6.3 权限和特权	100
6.3.1 用户和组管理工具	102
6.4 Windows 2000 NTFS	103
6.4.1 文件权限	103
6.4.2 默认安全设置	104
6.4.3 资源访问	106
6.4.4 特殊权限	106
6.4.5 与以前 NTFS 版本的区别	107
6.4.6 共享文件夹的发布：模糊中会有安全性吗？	108
6.5 默认注册表权限	108
6.6 软保护和 Windows 文件保护	110
6.6.1 软保护	110
6.6.2 Windows 文件保护	111
6.7 Windows 2000 加密文件系统	112
6.7.1 EFS 基础	112
6.7.2 加密文件系统如何工作	113
6.7.3 提供证书颁发机构的好处	114
6.7.4 Cipher 命令	115
6.7.5 恢复策略和 EFS 管理	116
6.8 最佳操作	116
6.9 更多的信息	117
6.10 小结	117
第7章 用户认证	118
7.1 LM 与 NTLM 认证	118
7.2 Windows 2000 中的 Kerberos	119

7.2.1 Kerberos 对 Windows 2000 的益处.....	119
7.2.2 活动目录的作用	120
7.2.3 认证的第 1 步: 获取登录会话密钥	120
7.2.4 认证的第 2 步: TGS 交换——获取特定服务器的票证	121
7.2.5 认证的第 3 步: 使用会话票证来获准进入——CS 交换	123
7.2.6 票证	123
7.2.7 DNS 名字解析	124
7.2.8 域间的活动	125
7.2.9 Kerberos 与 WinLogon 服务的集成	126
7.2.10 使用 Kerberos 票证来得到访问控制信息	128
7.2.11 Kerberos 与服务账号的集成	129
7.2.12 公钥的 Kerberos 扩展	130
7.3 网络登录的过程	131
7.4 在 Windows 2000 中使用智能卡	133
7.4.1 Microsoft 的方法	133
7.4.2 基本组件	134
7.4.3 安装与使用智能卡	135
7.4.4 使用智能卡进行 Windows 2000 登录	136
7.4.5 智能卡与远程访问	137
7.5 更多的信息	138
7.6 小结	138
第 8 章 生存周期选择	139
8.1 为了改进安全性而在安装时的注意事项	139
8.1.1 升级与全新安装之间的区别	140
8.1.2 保护升级安装的安全	141
8.1.3 已升级的 Windows NT 主域控制器 (PDC) 上的活动目录	141
8.2 维护	143
8.2.1 选择安全的应用程序: Windows 2000 应用程序标志的标准	143
8.2.2 使用和维护安全策略	147
8.2.3 备份	148
8.3 系统恢复: 修复概述	152
8.3.1 在安全模式中启动	152
8.3.2 紧急修复过程	153
8.3.3 使用最后一次正确配置	154
8.3.4 使用 Windows 2000 修复控制台	154
8.3.5 系统文件检查器	157
8.4 死亡与分解	158
8.5 最佳操作	158

8.6 更多的信息	159
8.7 小结	159
第9章 安全工具	160
9.1 使用安全配置和分析工具集	160
9.1.1 安全模板	161
9.1.2 安全配置和分析	162
9.1.3 使用 secedit 工具	165
9.1.4 使用安全配置工具集进行审核	167
9.2 组策略	167
9.2.1 组策略工具	168
9.2.2 GPO 组件	169
9.2.3 与组策略编辑器一起使用安全配置和分析	171
9.3 支持工具	171
9.4 Resource Kit 工具	171
9.4.1 与审核相关的工具	172
9.4.2 组策略工具	174
9.4.3 用户管理工具	176
9.4.4 管理工具	179
9.4.5 注册表工具	181
9.4.6 DACL	183
9.5 选择要使用的工具	186
9.6 最佳操作	187
9.7 更多的信息	187
9.8 小结	188
第10章 保护 Windows 2000 Professional 的安全	189
10.1 建立和保护用户和组数据库	189
10.1.1 安全模型	190
10.1.2 管理本地账号数据库中的账号和组	192
10.1.3 保护账号数据库	193
10.2 Windows NT 4.0 域中的 Windows 2000 Professional	194
10.2.1 Windows NT 4.0 域中的认证	195
10.2.2 Windows NT 域中的授权	195
10.3 使用组策略管理本地安全设置	196
10.3.1 账号策略	197
10.3.2 本地策略	197
10.3.3 策略设置	204
10.4 使安全设置与用户能力匹配	204

10.5 策略的实现和实施	205
10.5.1 密码策略	206
10.5.2 账号锁定	206
10.5.3 审核策略	206
10.5.4 用户权限	207
10.5.5 安全选项	207
10.5.6 事件日志设置	208
10.6 保护无线连接的安全	208
10.6.1 无线连接: 计算机与计算机	208
10.6.2 无线连接: 红外网络连接	209
10.7 安全数据和应用程序访问的协议与进程	209
10.8 使用 Windows 2000 Professional 管理 Windows 2000 域	210
10.8.1 可用的工具	210
10.9 最佳操作	211
10.10 更多的信息	211
10.11 小结	212
第 11 章 保护 Windows 2000 Server 的安全	213
11.1 Server 的角色	213
11.1.1 Server 的关系	213
11.1.2 Server 的作用	214
11.2 安装默认的安全项	216
11.2.1 用户和组	217
11.2.2 本地安全策略	217
11.3 策略设置	223
11.4 Server 安全模板	223
11.5 使用和保护终端服务	224
11.5.1 登录权限	225
11.5.2 应用程序问题	226
11.5.3 终端服务配置工具	226
11.5.4 数据加密	226
11.6 保护互操作服务	226
11.6.1 Macintosh 服务	227
11.6.2 Unix 服务	229
11.7 最佳操作	231
11.8 更多的信息	232
11.9 小结	233

第3部分 保护Microsoft本地局域网的安全

第 12 章 域级安全	234
12.1 活动目录概念介绍	234
12.1.1 活动目录层次	235
12.1.2 全局编录	238
12.1.3 信任关系	238
12.1.4 数据存储和复制	240
12.1.5 混合模式, 本机模式	240
12.1.6 LDAP	242
12.2 动态 DNS	242
12.2.1 动态 DNS 是怎样工作的	242
12.2.2 保护动态 DNS	245
12.3 分布式安全服务介绍	248
12.3.1 IPSec 策略	249
12.3.2 Kerberos 策略	250
12.4 网络认证服务的比较: Kerberos 和 NTLM	250
12.5 最佳操作	251
12.6 更多的信息	252
12.7 小结	252
第 13 章 保护传统 Windows 客户的安全	253
13.1 改善认证措施	253
13.1.1 下级客户的登录	253
13.1.2 实现 NTLMv2: 第一步——下级客户	256
13.1.3 实现 NTLMv2: 第二步——在 Windows 2000 域控制器上要求使用 NTLMv2	258
13.2 保护网络通信	258
13.2.1 SMB 签名	258
13.2.2 使用经协商的 NTLMv2 会话安全	260
13.3 改善基本的系统安全	261
13.3.1 系统策略编辑器	261
13.3.2 安全配置管理器	264
13.4 最佳操作	265
13.5 更多的信息	265
13.6 小结	266

第 14 章 保护分布式文件系统的安全	267
14.1 理解 DFS	267
14.1.1 定义、组件和概念	267
14.1.2 DFS 的工作方式	268
14.1.3 DFS 的使用	271
14.1.4 DFS 客户端	271
14.2 理解文件复制服务	271
14.2.1 定义 FRS 功能	271
14.2.2 在 DFS 中使用 FRS	272
14.2.3 管理 DFS 复制计划	273
14.3 保护 DFS 的安全	274
14.3.1 保护 DFS 拓扑结构	274
14.3.2 保护文件和文件夹	274
14.3.3 保护文件复制策略	275
14.3.4 规划安全的 DFS 架构	276
14.3.5 实现和维护	276
14.3.6 审核 DFS 的安全性	277
14.4 最佳操作	277
14.5 小结	278

第4部分 保护现实世界网络的安全

第 15 章 安全远程访问选项	279
15.1 路由和远程访问服务	279
15.1.1 网络地址转换和 Internet 连接共享	280
15.1.2 远程访问服务(RAS)	284
15.1.3 虚拟专用网络	289
15.2 Internet 认证服务	294
15.2.1 Internet 认证服务的配置和放置	295
15.2.2 IAS 策略	299
15.2.3 和 IAS 一起使用 VPN	300
15.2.4 什么时候使用 IAS, 什么时候使用 RRAS	300
15.3 终端服务	300
15.3.1 向用户提供远程访问	300
15.3.2 为管理员提供远程访问	301
15.4 保护远程管理访问的安全	301
15.4.1 使用策略控制访问	301
15.4.2 使用 telnet	302

15.5 最佳操作	302
15.6 更多的信息	302
15.7 小结	303
第 16 章 使用分布式安全服务保护网络的安全	304
16.1 活动目录操作	304
16.1.1 活动目录复制	305
16.1.2 保护活动目录	310
16.1.3 恢复活动目录	315
16.2 使用组策略对象控制计算机和用户	316
16.2.1 组策略处理	316
16.2.2 组策略继承	319
16.2.3 组策略管理的其他项目	323
16.2.4 组策略对象的复制和管理	326
16.2.5 策略应用	327
16.2.6 混合的 Windows 操作系统网络中的策略	328
16.2.7 组策略对象的权限委派	329
16.3 更多的信息	329
16.4 小结	329
第 17 章 企业公钥体系	330
17.1 Windows 2000 证书服务结构	330
17.1.1 证书颁发机构	331
17.1.2 证书层次	332
17.1.3 证书和证书模板	333
17.1.4 证书吊销列表	334
17.1.5 公钥策略	334
17.1.6 证书存储	334
17.1.7 加密服务提供者	335
17.1.8 证书信任列表	336
17.2 证书生存期	337
17.2.1 当安装根 CA 时, 颁发一份根 CA 证书	337
17.2.2 如果受到请求, 根 CA 可以为从属 CA 颁发证书	337
17.2.3 从属 CA 可以为别的从属 CA 颁发证书	337
17.2.4 周期性的发布证书吊销列表	337
17.2.5 根 CA 证书必须在过期之前或者整个证书服务结构失效之前重新颁发	338
17.2.6 从属 CA 证书在过期之前或者它颁发的任何证书失效之前重新颁发	338
17.2.7 证书请求放置在队列中等待管理员同意/拒绝	338
17.2.8 基于公钥体系的应用程序使用的证书	338