

精通

PKI

网络安全认证技术与编程实现

马臣云 王彦 编著

**PKI，利用公钥加密技术
解决电子商务信息安全需求的成熟体系**

内容充实，技术全面，覆盖了常见的PKI应用开发技术
注重应用，强调实战，填补了PKI类书籍只重理论没有实
战的空白

以“步骤 + 代码”的方式进行讲解，让初学者快速入门
实例典型、代码丰富，有极大的应用价值
博客专栏支持，解惑答疑，深入交流



人民邮电出版社
POSTS & TELECOM PRESS



CD-ROM

精通

PKI

网络安全认证技术与编程实现

马臣云 王彦 编著

精通PKI网络安全认证技术与编程实现

编著：马臣云、王彦

责任编辑：张博

人民邮电出版社出版发行

地址：北京市丰台区左安门内大街13号

邮编：100051

网址：<http://www.ptpress.com.cn>

北京顺义区牛栏山印刷厂印刷

开本：787×1092 1/16

印张：22.5

2008年7月第1版

字数：380千字

2008年7月北京第1次印刷

印数：1—5,000册

ISBN 978-7-113-07343-2

定价：22.00元（含邮费）

邮购地址：北京市丰台区左安门内大街13号（100051）
邮购电话：（010）67152492 邮购传真：（010）67152553

人民邮电出版社

北京

图书在版编目 (CIP) 数据

精通 PKI 网络安全认证技术与编程实现 / 马臣云, 王彦
编著. —北京: 人民邮电出版社, 2008.7
ISBN 978-7-115-17845-9

I. P… II. ①马…②王… III. ①计算机网络—安全技术②电子商务—安全技术 IV. TP393.08 F713.36

中国版本图书馆 CIP 数据核字 (2008) 第 035953 号

内 容 提 要

PKI 是解决开放式互联网络信息安全需求的成熟体系。PKI 体系支持身份认证, 信息传输、存储的完整性, 消息传输、存储的机密性, 以及操作的不可否认性。本书从实战出发, 介绍了 PKI 应用开发过程和细节。全书共 32 章, 分 6 篇, 主要内容包括 PKI 基础知识、OpenSSL 开发、CryptoAPI 开发、Java Security 开发、电子商务网站应用、PKI 技术应用等, 涉及 C 语言、Java 语言、JSP、ASP/ASP.NET、PHP 等开发语言。为了方便读者深入了解 PKI, 本书按照先原理、再讲解、再实战的方式进行, 并且全部实例和软件都保存在随书赠送的光盘中。

本书适合 PKI 应用开发人员、企业网络管理人员以及大、中专院校师生阅读。

精通 PKI 网络安全认证技术与编程实现

- ◆ 编 著 马臣云 王 彦
责任编辑 屈艳莲
- ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销
- ◆ 开本: 787×1092 1/16
印张: 29.25
字数: 766 千字
印数: 1—4 000 册
- 2008 年 7 月第 1 版
2008 年 7 月北京第 1 次印刷

ISBN 978-7-115-17845-9/TP

定价: 55.00 元 (附光盘)

读者服务热线: (010) 67132692 印装质量热线: (010) 67129223

反盗版热线: (010) 67171154

前言

随着电子商务的发展,网上购物、网上支付等消费方式已经逐渐被大众所接受。但是由于互联网的开放性,网络交易中的身份认证、数据保密、防篡改、防抵赖等安全需求变得越来越迫切。PKI(Public Key Infrastructure, 公开密码基础设施)是解决开放式互联网络信息安全需求的成熟体系。

PKI 是以现代密码学为基础的,其理论在国内外已经得到深入的研究。在我国,PKI 方面的应用也正在逐步开展,但是 PKI 开发人才的短缺极大地限制了其发展速度。

目前市场上有一些介绍 PKI 的中外文书籍,但都偏重于理论,或是与艰涩难懂的密码算法一起介绍。而本书直接从实战出发,介绍了 PKI 应用开发过程和细节。

本书介绍了 PKI 应用开发常用的技术,包括 OpenSSL 开发、CryptoAPI 开发、Java Security 开发、电子商务网站应用、PKI 相关技术应用等,涉及 C 语言、Java 语言、Web 开发语言(JSP、ASP/ASP.NET、PHP),每个系列都是按照先原理、再讲解、再实战的方式进行。力求读者学完本书后,可进行项目实践。

本书的特点

1. 技术全面,内容充实

本书覆盖了常见的 PKI 应用开发技术,包括 OpenSSL、CryptoAPI、Java Security、电子商务网站(JSP、ASP/ASP.NET、PHP)等。这样无论 Windows 开发还是 Web 开发,无论是 C 开发还是 Java 开发都可以从本书中获得必要的帮助。

2. 强调实战,示例代码丰富

本书在讲解知识点时,都附带了实例。每个章节在介绍函数后都会利用实例让读者深入了解该系列函数的功能和用法。同时,章节最后又包括了该部分项目级的综合应用。例如,讲解 OpenSSL 开发时,在 OpenSSL 加密和解密、消息摘要、签名验证等章节中都有相应的实例,最后又以 OpenSSL 的综合应用,即“文件保险箱”、“安全通信软件”、“安全报文系统”为例深入讲解,让读者了解项目级的 OpenSSL 开发情况。

3. 配有光盘，实例的源代码实际开发价值巨大

本书中涉及的全部实例都保存在附属光盘中，不少实例都是作者平时的项目积累，故源码的实际开发价值很大，稍微做些产品化即可完成实际项目需要。

4. 提供完善的售后服务

为了方便读者学习，作者在博客上创建一个专有版面：http://5233studio.bokee.com/catalog_60759.html。读者可以将自己遇到的问题发布在该版面上，我们将帮助大家解决这些问题。

本书的内容

第1篇（第1章）主要介绍 PKI 的基础知识。

第1章：介绍了什么是数字证书、为什么要使用数字证书、加密技术、数字签名技术。同时还介绍了常见的 PKI 术语。

第2篇（第2章~第11章）主要介绍了 OpenSSL 开发。

第2章：OpenSSL 入门介绍，包括 OpenSSL 概述、如何下载和编译 OpenSSL、如何搭建 OpenSSL 开发环境。

第3章：介绍了 OpenSSL 加密和解密，首先介绍了加解密的概念，然后详细介绍了相关函数的用法，并给出一个实例应用。

第4章：介绍了 OpenSSL 消息摘要，首先介绍了消息摘要的概念，然后介绍了相关函数的用法，并给出一个实例应用。

第5章：介绍了 OpenSSL 签名和验证，首先介绍了签名和验证的概念，然后介绍了相关函数的用法，并给出一个实例应用。

第6章：介绍了 OpenSSL Base64 编解和解码，首先介绍了 Base64 编解码的概念，然后介绍了相关函数的用法，并给出一个实例应用。

第7章：介绍了 OpenSSL 证书操作，首先介绍了证书的概念，然后介绍了相关函数的用法，并给出一个实例应用。

第8章：介绍了 OpenSSL SSL/TLS 编程，首先介绍了 SSL/TLS 的概念，然后介绍了相关函数的用法，并给出一个实例应用。

第9章：介绍了一个 OpenSSL 开发实例——文件保险箱，首先介绍了实例的功能，然后分析了实现流程，最后给出了功能实现的详细步骤。

第10章：介绍了一个 OpenSSL 开发实例——安全通信软件（SSL/TLS 通信），首先介绍了实例的功能，详细分析了实现流程，最后给出了功能实现的详细步骤。

第11章：介绍了一个 OpenSSL 开发实例——安全报文系统，首先介绍了实例的功能，然后分析了实现流程，最后给出了功能实现的详细步骤。

第3篇（第12章~第19章）主要介绍了 CryptoAPI 开发。

第12章：CryptoAPI 入门介绍，包括 CryptoAPI 组成、CryptoAPI 的优缺点和如何搭建开发环境。

第13章：介绍了 CryptoAPI 的密码服务提供者 CSP 函数，首先介绍了密码服务提供者的概念，然后介绍了相关函数的用法，并给出一个实例应用。

第14章：介绍了 CryptoAPI 的密钥的产生和交换函数，首先介绍了密钥的产生和交换函数

的概念, 然后介绍了相关函数的用法, 并给出一个实例应用。

第 15 章: 介绍了 CryptoAPI 的数据的加密和解密函数, 首先介绍了数据的加密和解密函数的概念, 然后介绍了相关函数的用法, 并给出一个实例应用。

第 16 章: 介绍了 CryptoAPI 的数据的哈希和数字签名函数, 首先介绍了哈希和数字签名函数的概念, 然后介绍了相关函数的用法, 并给出一个实例应用。

第 17 章: 介绍了 CryptoAPI 的证书和证书库函数, 首先介绍了证书和证书库函数的概念, 然后介绍了相关函数的用法, 并给出一个实例应用。

第 18 章: 介绍了一个 CryptoAPI 开发实例——文件保险箱, 首先介绍了实例的功能, 然后分析了实现流程, 最后给出了功能实现的详细步骤。

第 19 章: 介绍了一个 CryptoAPI 开发实例——安全报文系统, 首先介绍了实例的功能, 然后分析了实现流程, 最后给出了功能实现的详细步骤。

第 4 篇 (第 20 章~第 26 章) 主要介绍了 Java Security 开发。

第 20 章: Java Security 开发入门介绍, 包括 Java Security 设计原理和体系结构、主要概念、主要类和接口以及如何搭建开发环境。

第 21 章: 介绍了 Java 消息摘要, 首先介绍了 MessageDigest 类, 然后详细介绍了类内函数的用法, 并给出一个实例应用。

第 22 章: 介绍了 Java 加密和解密, 首先介绍了 KeyGenerator 和 Cipher 类, 然后详细介绍了类内函数的用法, 并给出一个实例应用。

第 23 章: 介绍了 Java 数字签名和验证, 首先介绍了 KeyPairGenerator 和 Signature 类, 然后详细介绍了类内函数的用法, 并给出一个实例应用。

第 24 章: 介绍了 keytool 和证书类, 首先介绍了 keytool 工具的使用方法以及参数的意义, 然后介绍了 X509Certificate 类、X509CRL 类的函数, 最后给出一个实例应用。

第 25 章: 介绍了一个 Java 开发实例——文件保险箱, 首先介绍了实例的功能, 然后分析了实现流程, 最后给出了功能实现的详细步骤。

第 26 章: 介绍了一个 Java 开发实例——安全报文系统, 首先介绍了实例的功能, 然后分析了实现流程, 最后给出了功能实现的详细步骤。

第 5 篇 (第 27 章~第 29 章) 主要介绍了 PKI 电子商务网站的应用。

第 27 章: 介绍 ASP/ASP.NET 电子商务网站应用, 包括 IIS 配置 SSL 服务器证书的方法、基于数字证书的用户身份认证、基于 CAPICOM 的数字签名应用、基于自开发控件的数字签名应用以及一个安全登录的实例。

第 28 章: 介绍 JSP 电子商务网站应用, 包括配置 JSP Web 服务器的 SSL 证书的方法、基于数字证书的用户身份认证、数字签名处理以及安全登录和订单签名两个实例。

第 29 章: 介绍 PHP 电子商务网站应用, 包括配置 Apache 的 SSL 证书的方法、基于数字证书的用户身份认证、数字签名处理以及安全登录和订单签名两个实例。

第 6 篇 (第 30 章~第 32 章) 主要介绍了 PKI 技术其他方面的应用。

第 30 章: 介绍如何颁发和获取数字证书, 包括利用 OpenSSL 颁发数字证书、利用 Windows 证书服务颁发数字证书、通过 CA 机构获取数字证书。

第 31 章: 介绍安全电子邮件应用, 分别介绍了 FoxMail 和 Outlook 的安全电子邮件的配置方法以及发送和阅读安全电子邮件的方法。

第 32 章: 介绍代码签名应用, 首先介绍了代码签名的概念, 然后分别介绍了 Windows 应用

程序代码签名、Java 代码签名、移动代码签名的操作方法。

适合的读者

- PKI 应用开发人员；
- C 程序员；
- JAVA 程序员；
- JSP Web 开发程序员；
- ASP Web 开发程序员；
- ASP.Net Web 开发程序员；
- PHP Web 开发程序员；
- 普通软件开发人员；
- 企业网络管理维护人员；
- 大、中专院校的师生；
- 社会培训学生。

关于作者

本书由马臣云组织编写，同时参与编写、资料整理和代码编写的有何世晓、何颖、卢顺科、吴恒奎、宋智广、宋燕、宋翔、寇苏朋、尚兴隆、张立全、戎剑、李东博、李丹、李春萌、杨涵、杨选举、梁其学、梁艺娟、苏鹏、陈励、鞠明君、黄志等，在此一并表示感谢。由于本书编写仓促，疏漏之处在所难免，望读者批评指正。

编 者

2008 年 5 月

目 录

第 1 篇 PKI 技术概述

第 1 章 PKI 基础知识.....	3	1.3.3 发送信息的不可否认性	5
1.1 PKI 概述	3	1.3.4 数据交换的完整性	6
1.2 什么是数字证书	3	1.4 加密技术	6
1.2.1 数字认证的原理	4	1.4.1 对称加密技术	6
1.2.2 数字认证是如何颁发的	5	1.4.2 非对称加密技术	7
1.3 为什么要使用数字证书	5	1.5 数字签名技术	8
1.3.1 信息传输的保密性	5	1.5.1 数字签名技术	8
1.3.2 交易者身份的确定性	5	1.5.2 时间戳技术	9

第 2 篇 OpenSSL 开发

第 2 章 OpenSSL 入门.....	13	2.3.2 Linux 下搭建 OpenSSL 开发 环境	22
2.1 OpenSSL 概述	13	2.4 小结	22
2.1.1 OpenSSL 的组成	13	第 3 章 OpenSSL 加密和解密	23
2.1.2 OpenSSL 的优缺点	14	3.1 概述	23
2.2 如何下载编译	15	3.2 函数介绍	23
2.2.1 Windows 下编译 OpenSSL	15	3.2.1 初始化函数 EVP_CIPHER_CTX_init	23
2.2.2 Linux 下编译 OpenSSL	17	3.2.2 加密初始化函数 EVP_EncryptInit_ex	24
2.3 如何搭建开发环境	19		
2.3.1 Windows 下搭建 OpenSSL 开发环境	19		

3.2.3 数据加密 Update 函数		5.1.5 验证 Update 函数	
EVP_EncryptUpdate	25	EVP_VerifyUpdate	41
3.2.4 数据加密结束函数		5.1.6 验证结束函数	
EVP_EncryptFinal_ex	25	EVP_VerifyFinal	41
3.2.5 解密初始化函数		5.2 实例应用	41
EVP_DecryptInit_ex	26	5.2.1 流程分析	42
3.2.6 数据解密 Update 函数		5.2.2 实例实现	44
EVP_DecryptUpdate	26		
3.2.7 数据解密结束函数		第 6 章 OpenSSL Base64 编解和解码	48
EVP_DecryptFinal_ex	27	6.1 函数介绍	48
3.3 实例应用——数据加密	27	6.1.1 Base64 编码初始化函数	
3.3.1 流程分析	27	EVP_EncodeInit	48
3.3.2 实例实现	28	6.1.2 Base64 编码 Update 函数	
		EVP_EncodeUpdate	48
第 4 章 OpenSSL 消息摘要	32	6.1.3 Base64 编码结束函数	
4.1 概述	32	EVP_EncodeFinal	49
4.2 函数介绍	32	6.1.4 Base64 编码函数	
4.2.1 初始化函数		EVP_EncodeBlock	49
EVP_MD_CTX_init	32	6.1.5 Base64 解码函数	
4.2.2 设置摘要算法函数		EVP_DecodeBlock	49
EVP_DigestInit_ex	33	6.1.6 Base64 解码初始化函数	
4.2.3 摘要 Update 函数		EVP_DecodeInit	50
EVP_DigestUpdate	33	6.1.7 Base64 解码 Update 函数	
4.2.4 摘要结束函数		EVP_DecodeUpdate	50
EVP_DigestFinal_ex	33	6.1.8 Base64 解码结束函数	
4.2.5 计算摘要函数		EVP_DecodeFinal	50
EVP_Digest	34	6.2 实例应用	50
4.3 实例应用	34	6.2.1 流程分析	51
4.3.1 流程分析	34	6.2.2 实例实现	52
4.3.2 实例实现	36		
第 5 章 OpenSSL 签名和验证	39	第 7 章 OpenSSL 证书操作	56
5.1 函数介绍	39	7.1 函数介绍	56
5.1.1 签名初始化函数		7.1.1 DER 编码转换为内部结构体	
EVP_SignInit_ex	39	函数 d2i_X509	56
5.1.2 签名 Update 函数		7.1.2 获得证书版本函数	
EVP_SignUpdate	40	X509_get_version	57
5.1.3 签名结束函数 EVP_SignFinal	40	7.1.3 获得证书序列号函数	
5.1.4 验证初始化函数		X509_get_serialNumber	58
EVP_VerifyInit_ex	40	7.1.4 获得证书颁发者信息函数	
		X509_get_issuer_name	58

7.1.5 获得证书拥有者信息函数		8.1.7 设置 SSL 私钥函数	
X509_get_subject_name.....	58	SSL_CTX_use_PrivateKey.....	75
7.1.6 获得证书有效期的起始日期		8.1.8 检查 SSL 私钥函数	
函数 X509_get_notBefore.....	59	SSL_CTX_check_private_key.....	75
7.1.7 获得证书有效期的终止日期		8.1.9 新建 SSL 句柄函数 SSL_new.....	76
函数 X509_get_notAfter.....	59	8.1.10 释放 SSL 句柄函数 SSL_free.....	76
7.1.8 获得证书公钥函数		8.1.11 设置 socket 句柄函数	
X509_get_pubkey.....	59	SSL_set_fd.....	76
7.1.9 创建和释放证书存储区函数 X509_		8.1.12 建立 SSL 链接函数	
STORE_new、X509_STORE_free.....	59	SSL_connect.....	76
7.1.10 向证书存储区添加证书函数		8.1.13 接受 SSL 链接函数	
X509_STORE_add_cert.....	59	SSL_accept.....	76
7.1.11 向证书存储区添加证书吊销		8.1.14 获得 SSL 链接使用的证书	
列表函数 X509_STORE_add_crl.....	60	SSL_get_peer_certificate.....	77
7.1.12 创建证书存储区上下文环境		8.1.15 发送 SSL 数据函数	
函数 X509_STORE_CTX_new.....	60	SSL_write.....	77
7.1.13 释放证书存储区上下文环境		8.1.16 读取 SSL 数据函数	
函数 X509_STORE_CTX_free.....	60	SSL_read.....	77
7.1.14 初始化证书存储区上下文环境		8.2 实例应用.....	77
函数 X509_STORE_CTX_init.....	60	8.2.1 流程分析.....	78
7.1.15 验证证书函数		8.2.2 实例实现.....	81
X509_verify_cert.....	61	第 9 章 开发实例——文件保险箱.....	89
7.2 实例应用.....	61	9.1 功能预览.....	89
7.2.1 流程分析.....	61	9.1.1 文件加密.....	89
7.2.2 实例实现.....	64	9.1.2 文件解密.....	90
第 8 章 SSL/TLS 编程.....	73	9.2 流程分析.....	91
8.1 函数介绍.....	73	9.2.1 文件加密函数 Encrypt_File.....	91
8.1.1 初始化 SSL 算法库函数		9.2.2 文件解密函数 Decrypt_File.....	93
SSL_library_init.....	73	9.3 功能实现.....	96
8.1.2 初始化 SSL 上下文环境变量函数		第 10 章 开发实例——安全通信	
SSL_CTX_new.....	74	软件.....	103
8.1.3 释放 SSL 上下文环境变量函数		10.1 功能预览.....	103
SSL_CTX_free.....	74	10.2 流程分析.....	105
8.1.4 设置 SSL 证书函数		10.2.1 服务端流程分析.....	105
SSL_CTX_use_certificate_file.....	74	10.2.2 客户端流程分析.....	109
8.1.5 设置 SSL 私钥函数		10.3 功能实现.....	112
SSL_CTX_use_PrivateKey_file.....	75	10.3.1 服务端.....	112
8.1.6 设置 SSL 证书函数		10.3.2 客户端.....	119
SSL_CTX_use_certificate.....	75		

第 11 章 开发实例——安全报文系统··· 126

11.1 功能预览····· 126

11.1.1 发送方产生安全报文····· 126

11.1.2 接收方解密安全报文····· 127

11.2 流程分析····· 129

11.2.1 发送方流程分析····· 129

11.2.2 接收方流程分析····· 133

11.3 功能实现····· 136

11.3.1 发送方····· 136

11.3.2 接收方····· 143

第 3 篇 CryptoAPI 开发

第 12 章 CryptoAPI 开发入门····· 153

12.1 CryptoAPI 的组成····· 154

12.2 CryptoAPI 的优缺点····· 154

12.3 如何搭建开发环境····· 154

第 13 章 密码服务提供者 CSP 函数····· 156

13.1 函数介绍····· 156

13.1.1 连接 CSP 函数

CryptAcquireContext····· 156

13.1.2 枚举 CSP 函数

CryptEnumProviders····· 157

13.1.3 获得默认 CSP 函数

CryptGetDefaultProvider····· 158

13.1.4 设置默认 CSP 函数

CryptSetProvider····· 158

13.1.5 获得 CSP 参数属性函数

CryptGetProvParam····· 158

13.1.6 设置 CSP 参数函数

CryptSetProvParam····· 159

13.1.7 断开 CSP 函数

CryptReleaseContext····· 160

13.2 实例应用····· 160

13.2.1 流程分析····· 160

13.2.2 实例实现····· 162

第 14 章 密钥的产生和交换函数····· 169

14.1 函数介绍····· 169

14.1.1 生成函数 CryptGenKey····· 169

14.1.2 派生密钥函数

CryptDeriveKey····· 170

14.1.3 销毁密钥函数

CryptDestroyKey····· 171

14.1.4 复制密钥函数

CryptDuplicateKey····· 171

14.1.5 导出密钥函数

CryptExportKey····· 171

14.1.6 导入密钥函数

CryptImportKey····· 171

14.1.7 获得密钥参数函数

CryptGetKeyParam····· 172

14.1.8 获得密钥参数函数

CryptSetKeyParam····· 173

14.1.9 获得密钥参数函数

CryptGenRandom····· 174

14.2 实例应用····· 174

14.2.1 流程分析····· 174

14.2.2 实例实现····· 178

第 15 章 数据的加密和解密函数····· 183

15.1 函数介绍····· 183

15.1.1 数据加密函数 CryptEncrypt··· 183

15.1.2 数据解密函数 CryptDecrypt··· 184

15.2 实例应用····· 184

15.2.1 流程分析····· 184

15.2.2 实例实现····· 188

第 16 章 哈希和数字签名函数····· 202

16.1 函数介绍····· 202

16.1.1 创建哈希函数

CryptCreateHash····· 202

16.1.2 销毁哈希

CryptDestroyHash····· 203

16.1.3 复制哈希函数

CryptDuplicateHash····· 203

16.1.4 获得哈希参数函数 CryptGetHashParam	203	17.1.7 获得证书句柄属性函数 Cert- GetCertificateContextProperty	221
16.1.5 设置哈希参数函数 CryptSetHashParam	204	17.1.8 设置证书句柄属性函数 Cert- SetCertificateContextProperty	221
16.1.6 哈希会话密钥函数 CryptHashSessionKey	204	17.1.9 获得证书主题名称函数 CertGetNameString	222
16.1.7 哈希数据函数 CryptHashData	205	17.2 实例应用	222
16.1.8 对哈希签名函数 CryptSignHash	205	17.2.1 流程分析	223
16.1.9 对哈希验证签名函数 CryptVerifySignature	206	17.2.2 实例实现	224
16.2 实例应用	206	第 18 章 开发实例——文件保险箱	228
16.2.1 流程分析	206	18.1 功能预览	228
16.2.2 实例实现	210	18.1.1 文件加密	228
第 17 章 证书和证书库函数	217	18.1.2 文件解密	229
17.1 函数介绍	217	18.2 流程分析	230
17.1.1 打开证书库函数 CertOpenStore	217	18.2.1 文件加密函数 Encrypt_File	230
17.1.2 关闭证书库函数 CertCloseStore	218	18.2.2 文件解密函数 Decrypt_File	234
17.1.3 从证书库枚举证书函数 CertEnumCertificatesInStore	219	18.3 功能实现	236
17.1.4 从证书库查找证书函数 CertFindCertificateInStore	219	第 19 章 开发实例——安全报文系统	246
17.1.5 创建证书句柄函数 CertCreateCertificateContext	220	19.1 功能预览	246
17.1.6 释放证书句柄函数 CertFreeCertificateContext	220	19.1.1 安全报文发送	247
		19.1.2 安全报文接收	248
		19.2 流程分析	249
		19.2.1 发送方流程分析	249
		19.2.2 接收方流程分析	255
		19.3 功能实现	259
		19.3.1 发送方	259
		19.3.2 接收方	267

第 4 篇 Java Security 开发

第 20 章 Java Security 开发入门	279	20.2.3 获得实现实例的 factory (工厂) 方法	282
20.1 设计原理和体系结构	279	20.3 主要类和接口	282
20.1.1 设计原理	279	20.4 搭建开发环境	282
20.1.2 体系结构	280	第 21 章 Java 消息摘要	283
20.2 主要概念	281	21.1 MessageDigest 类函数介绍	283
20.2.1 引擎类和算法	281	21.1.1 构造方法	283
20.2.2 实现和提供者	282		

21.1.2 生成实例对象函数	22.1.8 初始化密钥生成器函数
getInstance (1) 283	init (3) 293
21.1.3 生成实例对象函数	22.1.9 初始化密钥生成器函数
getInstance (2) 284	init (4) 293
21.1.4 获得密码服务提供者函数	22.1.10 初始化密钥生成器函数
getProvider 284	init (5) 294
21.1.5 计算摘要函数 update (1) 284	22.1.11 生成密钥函数 generateKey 294
21.1.6 计算摘要函数 update (2) 284	22.2 Cipher 类函数介绍 294
21.1.7 计算摘要函数 update (3) 285	22.2.1 构造方法 294
21.1.8 计算摘要函数 update (4) 285	22.2.2 生成实例对象函数
21.1.9 完成计算摘要函数 digest (1) 285	getInstance (1) 295
21.1.10 完成计算摘要函数	22.2.3 生成实例对象函数
digest (2) 285	getInstance (2) 295
21.1.11 完成计算摘要函数	22.2.4 获得密码服务提供者函数
digest (3) 286	getProvider 295
21.1.12 比较摘要值函数 isEqual 286	22.2.5 获得密码算法函数
21.1.13 对象重置函数 reset 286	getAlgorithm 295
21.1.14 获得摘要算法函数	22.2.6 获得密码算法分组长度函数
getAlgorithm 286	getBlockSize 296
21.1.15 获得摘要值长度函数	22.2.7 获得输出数据的长度函数
getDigestLength 287	getOutputSize 296
21.2 实例应用 287	22.2.8 获得初始化向量函数 getIV 296
21.2.1 流程分析 287	22.2.9 密码对象初始化函数
21.2.2 实例实现 288	init (1) 296
第 22 章 Java 加密和解密 291	22.2.10 密码对象初始化函数
22.1 KeyGenerator 类函数介绍 291	init (2) 297
22.1.1 构造方法 291	22.2.11 密码对象初始化函数
22.1.2 生成实例对象函数	init (3) 297
getInstance (1) 291	22.2.12 密码对象初始化函数
22.1.3 生成实例对象函数	init (4) 297
getInstance (2) 292	22.2.13 计算加密或解密函数
22.1.4 获得对象密码算法函数	update (1) 298
getAlgorithm 292	22.2.14 计算加密或解密函数
22.1.5 获得密码服务提供者函数	update (2) 298
getProvider 292	22.2.15 计算加密或解密函数
22.1.6 初始化密钥生成器函数	update (3) 299
init (1) 292	22.2.16 计算加密或解密函数
22.1.7 初始化密钥生成器函数	update (4) 299
init (2) 293	22.2.17 结束加密或解密函数
	doFinal (1) 300

22.2.18 结束加密或解密函数		23.2.10 更新签名或验证数据函数	
doFinal (2)	300	update (2)	310
22.3 实例应用	300	23.2.11 更新签名或验证数据函数	
22.3.1 流程分析	300	update (3)	310
22.3.2 实例实现	301	23.2.12 签名函数 sign (1)	310
第 23 章 Java 数字签名和验证	305	23.2.13 签名函数 sign (2)	310
23.1 KeyPairGenerator 类函数		23.2.14 验证签名函数 verify (1)	311
介绍	305	23.2.15 验证签名函数 verify (2)	311
23.1.1 构造方法	305	23.3 实例应用	312
23.1.2 获得密码算法函数		23.3.1 数字签名实现	312
getAlgorithm	305	23.3.2 数字签名验证实现	312
23.1.3 生成实例对象函数		23.3.3 实例实现	313
getInstance (1)	305	第 24 章 keytool 和证书类	317
23.1.4 生成实例对象函数		24.1 keytool 命令介绍	317
getInstance (2)	306	24.1.1 产生密钥对命令 genkey	317
23.1.5 密码对象初始化函数		24.1.2 向密钥仓库导入证书命令	
initialize (1)	306	import	318
23.1.6 密码对象初始化函数		24.1.3 导出证书请求命令 certreq	318
initialize (2)	306	24.1.4 导出证书命令 export	318
23.1.7 生成非对称密钥对函数		24.1.5 枚举仓库数据命令 list	319
genKeyPair 和 generateKeyPair	307	24.1.6 管理密钥仓库命令	
23.2 Signature 类函数介绍	307	storepasswd	319
23.2.1 构造方法	307	24.1.7 管理密钥仓库命令	
23.2.2 获得签名对象算法函数		keypasswd	319
getAlgorithm	307	24.1.8 管理密钥仓库命令 delete	319
23.2.3 生成实例对象函数		24.2 X509Certificate 类函数介绍	319
getInstance (1)	307	24.2.1 构造方法	319
23.2.4 生成实例对象函数		24.2.2 检查证书有效期函数	
getInstance (2)	308	checkValidity (1)	320
23.2.5 初始化验证对象函数		24.2.3 检查证书有效期函数	
initVerify (1)	308	checkValidity (2)	320
23.2.6 初始化验证对象函数		24.2.4 获得证书版本函数	
initVerify (2)	308	getVersion	320
23.2.7 初始化签名对象函数		24.2.5 获得证书序列号函数	
initSign (1)	309	getSerialNumber	320
23.2.8 初始化签名对象函数		24.2.6 获得证书颁发者函数	
initSign (2)	309	getIssuerX500Principal	321
23.2.9 更新签名或验证数据函数		24.2.7 获得证书主题信息函数	
update (1)	309	getSubjectX500Principal	321

24.2.8 获得证书有效起始日期函数 getNotBefore	321	24.3.11 获得 DER 编码的 CRL 信息函 数 getTBSCertList	324
24.2.9 获得证书有效期终止日期函数 getNotAfter	321	24.3.12 获得签名值函数 getSignature	325
24.2.10 获得 DER 编码的证书内容 函数 getTBSCertificate	321	24.3.13 获得签名算法名称函数 getSigAlgName	325
24.2.11 获得证书签名值函数 getSignature	321	24.4 实例应用	325
24.2.12 获得证书签名算法名称函数 getSigAlgName	322	24.4.1 流程分析	325
24.2.13 获得证书密钥用途函数 getKeyUsage	322	24.4.2 实例实现	326
24.3 X509CRL 类函数介绍	322	第 25 章 Java 开发实例——文件 保险箱	330
24.3.1 构造方法	322	25.1 功能预览	330
24.3.2 getEncoded	322	25.2 流程分析	332
24.3.3 验证 CRL 签名函数 verify	323	25.3 功能实现	333
24.3.4 获得 CRL 版本函数 getVersion	323	第 26 章 Java 开发实例——安全 报文系统	336
24.3.5 获得 CRL 颁发者函数 getIssuerX500Principal	323	26.1 功能预览	336
24.3.6 获得 CRL 本次更新时间函数 getThisUpdate	323	26.1.1 安全报文发送	336
24.3.7 获得 CRL 下次更新时间函数 getNextUpdate	324	26.1.2 安全报文接收	337
24.3.8 获得被吊销的证书函数 getRevokedCertificate (1)	324	26.2 流程分析	338
24.3.9 获得被吊销的证书函数 getRevokedCertificate (2)	324	26.2.1 发送方流程分析	338
24.3.10 获得被吊销的证书函数 getRevokedCertificate (3)	324	26.2.2 接收方流程分析	341
		26.3 功能实现	343
		26.3.1 密钥和证书 keystore 的 生成方法	343
		26.3.2 安全报文发送方	344
		26.3.3 安全报文接收方	348

第 5 篇 PKI 电子商务网站应用

第 27 章 ASP/ASP.Net 电子商务 网站应用	355	27.2 基于数字证书的用户身份认证	360
27.1 配置 IIS 的 SSL 服务器证书	355	27.2.1 基于数字证书的用户身份 认证的方法	361
27.1.1 生成证书请求	355	27.2.2 ASP/ASP.NET 页面获取客户端 证书的方法	361
27.1.2 安装证书	358	27.3 数据签名处理——基于 CAPICOM 的应用	366
27.1.3 启用 SSL	359		

27.3.1	CAPICOM 简介	366	27.6.2	签名页面后台 (Sign.aspx.cs)	389
27.3.2	CAPICOM 对象—— Certificate 对象	367	27.6.3	验证签名页面前台 (verifySign.aspx)	389
27.3.3	CAPICOM 对象—— Certificates 对象	369	27.6.4	验证签名后台页面 (verifySign.aspx.cs)	390
27.3.4	CAPICOM 对象—— CertificateStatus 对象	369	27.7	小结	394
27.3.5	CAPICOM 对象—— Store 对象	370	第 28 章	JSP 电子商务网站应用	395
27.3.6	CAPICOM 对象—— SignedData 对象	372	28.1	配置 JSP Web 服务器的 SSL 证书	395
27.3.7	CAPICOM 对象—— Signer 对象	374	28.1.1	生成证书请求文件 (CSR)	395
27.3.8	CAPICOM 对象—— Signers 对象	374	28.1.2	导入证书	397
27.3.9	CAPICOM 对象—— EnvelopedData 对象	374	28.1.3	设置 Tomcat 支持 SSL	397
27.3.10	CAPICOM 对象—— Recipients 对象	375	28.1.4	使用浏览器访问 SSL 服务器	398
27.3.11	CAPICOM 对象—— Algorithm 对象	375	28.2	基于数字证书的用户身份认证	398
27.3.12	CAPICOM 对象—— 其他对象	376	28.2.1	基于数字证书的用户身份 认证的方法	399
27.3.13	如何在客户端安装部署和 调用	376	28.2.2	JSP 页面获取客户端证书的 方法	399
27.3.14	如何在服务器端安装部署和 调用	377	28.3	数据签名处理	401
27.4	基于自开发控件应用	378	28.3.1	JSP 前台提交签名	401
27.4.1	开发 ActiveX 控件	378	28.3.2	JSP 后台处理签名	402
27.4.2	如何在客户端部署和调用	383	28.4	开发实例——安全登录	403
27.4.3	代码示例	384	28.4.1	SSL 登录处理页面 (login.jsp)	404
27.5	开发实例——安全登录	385	28.4.2	用户主页面 (main.jsp)	405
27.5.1	登录处理页面 (login.aspx.cs)	385	28.4.3	出错处理页面 (err.jsp)	405
27.5.2	用户页面 (main.aspx.cs)	386	28.4.4	测试代码	405
27.5.3	出错显示页面 (err.aspx.cs)	387	28.5	开发实例——订单签名	406
27.5.4	测试功能	387	28.5.1	签名页面 (Sign.jsp)	406
27.6	开发实例——订单签名	388	28.5.2	验证签名页面 (verifySign.jsp)	407
27.6.1	签名页面前台 (Sign.aspx)	388	第 29 章	PHP 电子商务网站应用	410
			29.1	配置 Apache 的 SSL 证书	410
			29.1.1	安装 Apache+PHP+SSL	410
			29.1.2	配置 Apache 的 SSL 证书	412
			29.2	基于数字证书的用户身份认证	414

29.2.1 基于数字证书的用户身份认证的方法	414
29.2.2 PHP 页面获取客户端证书的方法	415
29.3 数据签名处理	417
29.3.1 PHP 前台提交签名	417
29.3.2 PHP 后台处理签名	419
29.4 开发实例——安全登录	423
29.4.1 登录页面 (login.php)	423
29.4.2 用户主页面 (main.php)	424
29.4.3 出错处理页面 (err.php)	424
29.4.4 测试代码	424
29.5 开发实例——订单签名	425
29.5.1 签名页面 (Sign.php)	425
29.5.2 验证签名页面 (verifySign.php)	426
29.5.3 测试代码	427

第6篇 其他 PKI 技术应用

第30章 颁发和获取数字证书	431
30.1 利用 OpenSSL 颁发数字证书	431
30.1.1 准备工作	431
30.1.2 建立根证书	431
30.1.3 颁发用户证书	433
30.2 利用 Windows 证书服务颁发数字证书	434
30.2.1 准备工作	434
30.2.2 安装证书服务并设置 CA	434
30.2.3 提交证书请求	435
30.2.4 证书颁发机构处理请求	436
30.2.5 下载证书	437
30.3 通过 CA 机构获取数字证书	438
第31章 安全电子邮件应用指南	439
31.1 Foxmail 安全电子邮件应用	439
31.1.1 为 Foxmail 邮箱账户配置证书	439
31.1.2 发送和阅读安全电子邮件	440
31.2 Outlook 安全电子邮件应用	441
31.2.1 为 Outlook 邮箱账户配置证书	441
31.2.2 发送和阅读安全电子邮件	442
第32章 代码签名应用指南	445
32.1 什么是代码签名	445
32.2 Windows 应用程序代码签名	445
32.2.1 申请代码签名证书	445
32.2.2 使用 SignCode.exe 对代码签名	446
32.2.3 查看代码签名证书	449
32.3 Java 代码签名	449
32.3.1 下载签名工具	449
32.3.2 申请签名证书	449
32.3.3 执行代码签名	450
32.3.4 验证 Java 代码签名	450
32.4 移动代码签名	450
32.4.1 主流移动操作系统对代码签名的要求	450
32.4.2 代码签名的操作方法	451