

E-commerce

电子商务核心技术

——安全电子交易协议的理论与设计

■ 梁施 晋仁
王育民 编著
梁峰
刘哲



西安电子科技大学出版社

[http:// www.xduph. com](http://www.xduph.com)

电子商务核心技术

——安全电子交易协议的理论与设计

梁 晋 施 仁 编著
王育民 梁 峰 刘 哲

西安电子科技大学出版社

2 0 0 0

内容简介 电子商务是目前 Internet 发展的热点,支付协议是电子商务的核心问题。以安全电子交易协议(SET)为代表的支付方式和协议逐渐被人们所熟悉。SET 协议是目前支付协议中最为复杂的标准,涉及电子商务、密码理论、计算机网络技术等各方面的知识。目前国内有关电子商务的介绍性书籍不少,但有关电子商务支付协议的技术资料却不多。本书立足 SET 协议的理论和设计,向读者全面系统地讲解了目前电子商务支付系统的理论和设计技术,重点是 SET 协议的标准和扩展技术。通过本书的学习,读者不但能够对 SET 协议有较深刻的理解,并且能够熟悉其它支付协议和标准。

全书分七部分。第一部分综述电子商务支付系统和 SET 协议;第二部分是有关 SET 的安全和密码理论知识;第三部分是 SET 协议设计综述;第四部分是 SET 协议的证书管理;第五部分是 SET 协议的支付管理;第六部分是 SET 协议的接口扩展;第七部分是支付系统的探讨和 SET 协议的最新扩展,对比了 SSL 协议,介绍了目前 SET 的最新扩展,以及微支付方式。

本书可作为有关专业的大学本科或研究生教材,也是有关计算机和网络行业从业人员进行电子商务设计、研究和开发的有价值的参考资料。

图书在版编目(CIP)数据

电子商务核心技术:安全电子交易协议的理论与设计/梁晋等编著. —西安:西安电子科技大学出版社,2000.8

ISBN 7-5606-0894-9

I. 电… II. 梁… III. 计算机网络—商业经营—支付方式—安全—协议 IV. F713.36

中国版本图书馆 CIP 数据核字(2000)第 35257 号

责任编辑 李惠萍 殷威安

出版发行 西安电子科技大学出版社(西安市太白南路 2 号)

电 话 (029)8227828 邮 编 710071

http://www.xduph.com E-mail: xdupfxb@pub.xaonline.com

经 销 新华书店

印 刷 陕西画报社印刷厂

版 次 2000 年 8 月第 1 版 2000 年 8 月第 1 次印刷

开 本 787 毫米×1092 毫米 1/16 印张 30

字 数 704 千字

印 数 1~4000 册

定 价 36.00 元

ISBN 7-5606-0894-9/TP·0476

* * * 如有印装问题可调换 * * *

本书封面贴有西安电子科技大学出版社的激光防伪标志,无标志者不得销售。

前

言

电子商务的发展将计算机技术(特别是 Internet 技术)拓展到社会各个领域。电子商务的一个核心问题是支付,目前比较流行的支付协议有 SSL、SET 等。SSL 比较简单,应用得比较多,但其问题也比较多,发展潜力不大。在本书第十九章对 SSL 和 SET 作了详细比较。SET 协议在商业上得到了 VISA 和 MASTER 等大的支付卡品牌的支持,在技术上得到了计算机大厂商(如 IBM、Microsoft、HP 等)的支持,是目前支持力量最大的支付协议。虽然 SET 协议从 1997 年正式公布以来,其应用存在一些问题,迫使 SET 协议的标准组织 SETCo 在 1998 年和 1999 年提出了许多 SET 协议扩展,这些扩展针对 SET 协议在应用中出现的作了一些改进,如支持 IC 卡、智能卡、借记卡;对商家和持卡者之间支持非 SET 消息,如持卡者可以通过电话、传真、SSL 等非 SET 协议进行交易。这些扩展的推出解决了 SET 协议应用中的一些问题。另外,在电子商务中还有许多支付协议和方式,如目前兴起的微支付方式。在本书第 21 章,将对微支付协议进行介绍。

一、本书读者对象

1. 相关专业的工程技术人员

这些读者可能比较关心如何建立一套电子商务系统,而不是开发一个 SET 应用程序。此类读者需要详细阅读本书,但因为只有了解了支付协议的内容,才能有效地建立支付系统。例如,即使用户买了一套 SET 支付软件,如 IBM 的 Net.commerce,但因为 SET 协议有许多可变因素和扩展协议,不了解消息协议也很难进行应用。

2. 研究和开发人员

对于研究和开发人员,在阅读本书的基础上,建议读者阅读 SET 协议的 ANSI.1 表示,也就是“SET Secure Electronic Transaction Specification Book 3: Formal Protocol Definition Version 1.0”。

3. 计算机爱好者

有些计算机爱好者,能够熟练操作计算机和上网,对于这些读者,第二部分可以不看,只阅读其它部分内容即可。

二、本书的内容安排

本书以 SET 协议为线索,分为七个部分。如果读者没有密码方面的知识,建议读者先对第二部分网络安全和密码理论作一了解,再阅读其余部分。

第一部分 电子商务和支付介绍

本部分介绍电子商务和支付系统的概念,对 SET 协议作总体描述,包括第 1、2 章。第 1 章 电子商务和支付系统概述,第 2 章 SET 协议的总述,介绍 SET 的概念和支付处理流程。

第二部分 网络安全和密码理论

该部分介绍网络安全和密码理论基础,介绍 SET 协议涉及的安全密码理论,包括第 3~7 章。第 3 章 信息网络安全概述,第 4 章 密码理论基础,第 5 章 对称密钥密码技术,第 6 章 公钥密码技术,第 7 章 公开密钥基础设施(PKI)。

第三部分 SET 系统设计综述

该部分介绍涉及 SET 的开发工具和应用的考虑事项,提供背景信息,介绍突出的特性,包括第 8~10 章。第 8 章 SET 系统设计介绍,第 9 章 SET 技术要求,第 10 章 SET 系统概念。

第四部分 SET 协议证书管理

本部分介绍有关 SET 协议的证书管理结构、协议、概念等,包括第 11~13 章。第 11 章 证书管理结构,第 12 章 证书格式,第 13 章 证书请求协议。

第五部分 SET 支付系统

本部分介绍 SET 协议中有关支付系统的处理和描述,包括所有与授权、付款和支付系统管理有关的所有消息,包括第 14~16 章。第 14 章 SET 一般数据和流程,第 15 章 持卡者和商家消息,第 16 章 商家与支付网关的消息。

第六部分 SET 协议的外部接口指导

该部分不是 SET 协议的本身,而是为开发者提供开发交互操作应用程序的指导。主要介绍 SET 协议没有详细定义的初始消息和传输机制,包括第 17、18 章。第 17 章 SET 初始消息,第 18 章 传输机制。

第七部分 电子商务支付系统探讨

本部分主要是有关 SET 协议的讨论和分析,对比了 SSL 协议,介绍了目前 SET 的最新扩展,以及微支付方式,包括第 19~21 章。第 19 章 SSL 及 SET 分析,第 20 章 SET 协议扩展及发展趋势,第 21 章 Internet 微支付及其它。

本书主要作者梁晋,博士毕业,现为西安交通大学的教师,工作于西安交通大学信息机电研究所,是中国信息经济学会电子商务分会的常务理事。另两位作者施仁教授、梁峰老师都工作于西安交通大学电子与信息工程学院。王育民教授是西安电子科技大学的老师,也是我国密码安全专家。刘哲是陕西邮电管理局技术人员。同时,本书的编写得到了西安凯辉电子有限责任公司的大力支持。

目前,国外对电子商务支付的研究和产品较多,而国内还处在初级阶段,有关支付系统深层次的技术资料很少,产品研究基本处于空白状态。希望本书能为国内电子商务支付系统的研究提供帮助。

书中错误之处请读者批评指正。

作者梁晋 E-mail: jin_liang@netease.com.

作 者

2000 年 2 月 5 日

于西安交通大学

目 录

第一部分 电子商务和支付介绍

第 1 章 电子商务和支付系统概述	2
1.1 电子商务介绍	2
1.1.1 电子商务的特性	2
1.1.2 电子商务发展过程	3
1.1.3 电子商务的分类	5
1.1.4 电子商务是一个新的产业革命	7
1.1.5 电子商务的价值和功能	8
1.1.6 电子商务应用系统的构成	10
1.2 电子商务和支付系统的选择	12
1.2.1 支付服务	13
1.2.2 支付类型	13
1.2.3 支付模型选择标准	16
1.2.4 购买和支付环境	17
1.3 电子商务安全性要求和支付交易协议	19
1.3.1 电子商务安全问题	19
1.3.2 电子商务采用的主要安全技术及其标准规范	20
1.3.3 现有电子商务交易协议	24
1.3.4 在线交易主要模式	25
第 2 章 SET 协议的总述	29
2.1 SET 协议介绍	29
2.1.1 SET 技术标准	30
2.1.2 SET 扩展规范	31
2.1.3 SET 采用的外部标准	31
2.2 基本概念	33
2.2.1 支付系统参与者(Payment System Participants)	33
2.2.2 加密概念	33
2.3 证书发行(Certificate Issuance)	38
2.4 购物类型	39
2.5 支付处理(Payment Processing)	40
2.5.1 持卡者注册(Cardholder Registration)	41
2.5.2 商家注册(Merchant Registration)	44

2.5.3 购买请求(Purchase Request)	45
2.5.4 支付授权(Payment Authorization)	46
2.5.5 支付请款(Payment Capture)	48

第二部分 网络安全和密码理论

第3章 信息网络安全概述 50

3.1 网络的安全策略	50
3.2 安全威胁与防护措施	52
3.2.1 安全威胁	52
3.2.2 防护措施	54
3.3 网络安全业务	55
3.3.1 认证	55
3.3.2 访问控制	56
3.3.3 保密	57
3.3.4 数据完整性	57
3.3.5 不可否认	58
3.4 信息安全标准	59

第4章 密码理论基础..... 66

4.1 保密学的基本概念	67
4.2 密码体制分类	68
4.3 初等密码分析	70
4.4 信息论与密码学介绍	72
4.5 密码与计算复杂性关系	72
4.6 实际保密性	74

第5章 对称密钥密码技术 76

5.1 流密码	76
5.2 拟随机数生成器的一般理论	77
5.3 分组密码理论与技术	79
5.3.1 分组密码概述	80
5.3.2 美国数据加密标准 DES	83
5.3.3 分组密码运行模式	87
5.3.4 其它分组密码	89

第6章 公钥密码技术..... 92

6.1 公开密钥密码概述	92
6.2 公钥密码体制	95
6.2.1 双钥密码体制的基本概念	95
6.2.2 RSA 密码体制	98

6.2.3 椭圆曲线密码体制	99
6.2.4 其它公钥体制	101
6.3 Hash 杂凑函数	101
6.3.1 单向杂凑函数	102
6.3.2 杂凑函数的安全性	103
6.3.3 MD-4 和 MD-5 杂凑算法	104
6.3.4 安全杂凑算法(SHA)	104
6.3.5 其它 Hash 算法	108
6.4 数字签字	109
6.4.1 数字签字基本概念	109
6.4.2 RSA 签字体制	110
6.4.3 DSS 签字标准	111
6.4.4 其它签字方式	112
第 7 章 公开密钥基础设施(PKI)	115
7.1 PKI 概述	115
7.1.1 PKI 的功能	118
7.1.2 PKI 的性能要求	118
7.2 PKI 的基本特征	119
7.2.1 证书的类型及内容	120
7.2.2 PKI 的各个 CA、证书主体(Subject)及证书用户三者之间的关系	120
7.2.3 CA 的排列	120
7.2.4 证书确认的方法	122
7.2.5 证书废止	122
7.2.6 强身份认证和非否认	123
7.2.7 匿名	123
7.3 基于 X.509 的 PKI	124
7.3.1 X.500	124
7.3.2 X.509 V1 和 V2	125
7.3.3 X.509 V3	126
7.3.4 X.509 V3 凭据证书	129
7.3.5 X.509 的 PKI 基本特征	129

第三部分 SET 系统设计综述

第 8 章 SET 系统设计介绍	131
8.1 背景信息	131
8.1.1 使用范围	132
8.1.2 环境	133
8.2 转账付款处理	135
8.2.1 终端数据请款	136

8.2.2 主机数据请款	137
8.3 商业付款流程	138
8.4 系统综述	141
8.5 SET 安全服务	143
8.5.1 服务分类	143
8.5.2 证书	143
8.5.3 品牌的证书撤销列表标识(Brand CRL Identifier)	145
第 9 章 SET 技术要求	146
9.1 SET 安全性	146
9.1.1 机密性(Confidentiality)	146
9.1.2 认证	146
9.1.3 数据完整性	147
9.2 SET 适应性	148
9.3 SET 交互性	148
9.3.1 消息封装(Message Wrapper)	149
9.3.2 向后兼容性(Backwards Compatibility)	150
9.3.3 SET 消息的扩展机制	151
9.3.4 PKCS #7 格式	151
9.3.5 非 SET 系统的交易验证	153
第 10 章 SET 系统概念	154
10.1 概述	154
10.1.1 符号和定义	154
10.1.2 加密技术	157
10.1.3 缩写词(Acronyms)	160
10.2 其它特征	162
10.2.1 幂等性(Idempotency)	162
10.2.2 特别数据区类型(Special Field Types)	163
10.2.3 根公用密钥的分发(Root Public Key Distribution)	163
10.2.4 非在线证书(Off-line Certificates)	164
10.2.5 Cert-PE	164
10.3 SET 加密处理步骤	164
10.3.1 发送消息(Send Message)	165
10.3.2 接收消息(Receive Message)	165
10.3.3 证书链验证(Certificate Chain Validation)	166
10.3.4 指纹(Thumbprints)	166
10.3.5 带签字的简单封装(Simple Encapsulation with Signature)	167
10.3.6 带签字和密钥的简单封装(Simple Encapsulation with Signature and Provided Key)	167
10.3.7 带签字的额外封装(Extra Encapsulation with Signature)	168
10.3.8 带签字和行李的简单封装(Simple Encapsulation with Signature and Baggage)	168
10.3.9 带签字和行李的额外封装(Extra Encapsulation with Signature and Baggage)	168
10.3.10 非对称加密(Asymmetric Encryption)	169

10.3.11	具有完整性的非对称加密(Asymmetric Encryption with Integrity)	169
10.3.12	非对称额外加密(Extra Asymmetric Encryption)	170
10.3.13	具有完整性的非对称额外加密(Extra Asymmetric Encryption with Integrity)	170
10.3.14	对称加密(Symmetric Encryption)	171
10.3.15	签字(Signature)	171
10.3.16	仅签字(Signature Only)	173
10.3.17	密钥 Hash(Keyed - Hash)	173
10.3.18	杂凑(Hash)	173
10.3.19	摘要数据(Digested Data)	173
10.3.20	链接(Linkage)	174
10.3.21	最优非对称加密填充(Optimal Asymmetric Encryption Padding)	174
10.4	SET 错误处理	176

第四部分 SET 协议证书管理

第 11 章	SET 证书管理结构	181
11.1	证书管理结构概述	181
11.2	证书管理的功能概述	183
11.2.1	证书发行(Certificate Issuance)	183
11.2.2	证书更新(Certificate Renewal)	184
11.2.3	证书撤消(Certificate Revocation)	184
11.3	证书链确认(Certificate Chain Validation)	185
11.3.1	证书链的验证(Validation of Certificate Chain)	185
11.3.2	证书中的日期(Dates in Certificates)	186
11.3.3	指纹(Thumbprints)	187
11.4	根证书分发(Root Certificate Distribution)	188
11.5	证书撤消	189
第 12 章	证书格式	191
12.1	X.509 证书定义	191
12.1.1	X.509 证书数据定义(Certificate Data Definitions)	191
12.1.2	证书主体名称格式(Certificate Subject Name Format)	192
12.1.3	名称区(Name Fields)	194
12.2	X.509 扩展	195
12.2.1	AuthorityKeyIdentifier 扩展	195
12.2.2	KeyUsage 扩展	196
12.2.3	PrivateKeyUsagePeriod 扩展	197
12.2.4	CertificatePolicies 扩展	198
12.2.5	SubjectAltName 扩展	201
12.2.6	BasicConstraints 扩展	201

12.2.7	IssuerAltName 扩展	202
12.3	SET 私用扩展(SET Private Extensions)	203
12.3.1	HashedRootKey 私用扩展	203
12.3.2	CertificateType 私用扩展	204
12.3.3	MerchantData 私用扩展	205
12.3.4	CardCertRequired 私用扩展	207
12.3.5	隧道私用扩展(Tunneling Private Extension)	207
12.3.6	SETExtensions 扩展	208
12.4	证书类型总结	209
12.5	证书撤销列表和 BCI	211
12.5.1	X.509 CRL 数据定义	211
12.5.2	CRL 扩展	213
12.5.3	CRL 确认	213
12.5.4	BrandCRLIdentifier	213
第 13 章	证书请求协议	216
13.1	证书请求主要协议	216
13.1.1	证书请求协议要求的数据和处理	216
13.1.2	主要协议的详细描述	218
13.2	协议变化(Protocol Variations)	219
13.3	持卡人证书初始请求和响应处理	220
13.3.1	持卡人产生证书初始请求消息(Cardholder Generates CardCInitReq)	221
13.3.2	CCA 处理持卡人证书初始化请求(CCA Processes CardCInitReq)	221
13.3.3	CCA 产生持卡人证书响应(CCA Generates CardCInitRes)	222
13.3.4	持卡人处理证书初始化响应(Cardholder Processes CardCInitRes)	222
13.4	持卡人注册表请求和响应处理	223
13.4.1	持卡人产生注册表请求 RegFormReq	223
13.4.2	CCA 产生 RegFormRes 响应消息	225
13.5	商家/支付网关证书初始处理	228
13.5.1	商家/支付网关产生 Me - AqCInitReq	228
13.5.2	CA 产生 Me - AqCInitRes	230
13.5.3	商家或收单行处理 Me - AqCInitRes	232
13.6	证书请求和产生处理	232
13.6.1	最终实体产生 CertReq(End Entity Generates CertReq)	232
13.6.2	CA 验证 CertReq	238
13.6.3	金融机构认证	240
13.6.4	CA 产生证书响应 CertRes	240
13.6.5	最终实体处理 CertRes	243
13.7	证书查询和状态处理	244
13.7.1	最终实体产生 CertInqReq	244
13.7.2	CA 产生 CertInqRes	245
13.8	CA 和 CA 消息	245
13.8.1	证书请求和响应	245

13.8.2 CRL 分发	247
13.8.3 BCI 恢复	248

第五部分 SET 支付系统

第 14 章 SET 一般数据和流程	251
14.1 数据结构(Data Structures)	251
14.1.1 交易标识(TransIDs)	251
14.1.2 支付指示 PI	254
14.1.3 分期付款和定期付款数据(InstallRecurData)	255
14.1.4 授权标记(AuthToken)	256
14.1.5 收单行发出的支付卡消息(AcqCardMsg)	257
14.1.6 请款标记(CapToken)	258
14.1.7 主账号数据(PANData)	259
14.1.8 账号标记(PANToken)	260
14.1.9 详细销售(SaleDetail)	260
14.1.10 请求和响应消息标签(RRTags)	267
14.1.11 批状态(BatchStatus)	268
14.1.12 交易详细信息(TransactionDetail)	269
14.1.13 金额数量数据区(Amount Fields)	270
14.1.14 日期参数(Date Fields)	270
14.2 消息一般流程	270
第 15 章 持卡者和商家消息	273
15.1 支付初始化请求和响应处理	273
15.1.1 PInitReq 消息的产生和处理	274
15.1.2 初始化响应 PinitRes 的产生和处理	275
15.1.3 扩展指导(Extension Guidelines)	277
15.2 购买订购请求和响应处理(Purchase Order Request/Response Processing)	277
15.2.1 持卡者产生 PReq	278
15.2.2 商家产生购买响应 PRes	282
15.2.3 扩展指导	286
15.3 查询请求响应处理(Inquiry Request/Response)	287
第 16 章 商家与支付网关的消息	289
16.1 授权请求和响应(Authorization Request/Response)	289
16.1.1 商家产生 AuthReq	290
16.1.2 支付网关产生授权响应(Payment Gateway Generates AuthRes)	294
16.1.3 提示处理(Referral Processing)	298
16.1.4 扩展指导(Extension Guidelines)	299
16.2 授权撤消(Authorization Reversal)	299

16.2.1	商家产生授权撤销请求(Merchant Generates AuthRevReq)	300
16.2.2	支付网关产生授权撤销响应(Payment Gateway Generates AuthRevRes)	302
16.2.3	扩展指导(Extension Guidelines)	304
16.3	请款请求和响应(Capture Request/Response)	304
16.3.1	商家产生请款请求(Merchant Generates CapReq)	304
16.3.2	支付网关产生请款响应(Payment Gateway Generates CapRes)	307
16.3.3	扩展指导(Extension Guidelines)	310
16.4	请款撤销或退款数据(Capture Reversal or Credit Data)	311
16.4.1	商家产生 CapRevOrCredReqData	311
16.4.2	支付网关产生 CapRevOrCredRes 响应数据	313
16.4.3	扩展指导(Extension Guidelines)	316
16.5	请款撤销(Capture Reversal)	316
16.6	退款请求和响应(Credit Request/Response)	318
16.6.1	商家产生退款请求(Merchant Generates CredReq)	318
16.6.2	支付网关产生退款响应(Payment Gateway Generates CredRes)	319
16.7	退款撤销请求和响应(Credit Reversal Request/Response)	320
16.7.1	商家产生退款撤销请求(Merchant Generates CredRevReq)	320
16.7.2	支付网关产生退款撤销响应(Payment Gateway Generates CredRevRes)	321
16.8	支付网关证书请求和响应(Gateway Certificate Request/Response)	322
16.8.1	商家产生支付网关证书请求(Merchant Generates PCertReq)	322
16.8.2	支付网关产生网关证书响应(Payment Gateway Generates PCertRes)	323
16.8.3	扩展指导(Extension Guidelines)	325
16.9	批管理(Batch Administration)	325
16.9.1	商家产生批管理请求(Merchant Generates BatchAdminReq)	326
16.9.2	支付网关产生批管理响应(Payment Gateway Generates BatchAdminRes)	331
16.9.3	扩展指导(Extension Guidelines)	333

第六部分 SET 协议的外部接口指导

第 17 章	SET 初始消息	335
17.1	介绍	335
17.1.1	术语	335
17.1.2	SET 初始发行信息(SET Initiation Issues)	336
17.2	MIME 介绍	338
17.2.1	消息头(Message Header)	338
17.2.2	MIME 消息体	339
17.2.3	MIME 中定义的 SET 内容类型	339
17.3	SET 初始消息结构	340
17.3.1	初始消息头数据区类型(Initiation Message Header Field Types)	341
17.3.2	通用初始头数据区(Common Initiation Header Fields)	342
17.4	注册初始消息(Registration Initiation Messages)	346

17.4.1	持卡者注册(Cardholder Registration)	347
17.4.2	商家和支付网关注册(Merchant and Payment Gateway Registration)	347
17.4.3	注册初始消息头(Registration - Initiation Message Header)	348
17.4.4	注册查询初始消息头(Registration - Inquiry - Initiation Message Header)	349
17.5	支付初始消息	350
17.5.1	持卡者支付(Cardholder Payment)	350
17.5.2	支付初始消息的头(Payment - Initiation Message Header)	351
17.5.3	支付初始消息体(Payment - Initiation Message Body)	353
17.5.4	支付初始消息举例	353
17.5.5	支付查询初始消息的头(Payment - Inquiry - Initiation Message Header)	354
17.6	初始响应消息(Initiation Response Message)	356
第 18 章	传输机制	359
18.1	World Wide Web 操作介绍	359
18.1.1	信息发行	359
18.1.2	WWW 交互作用	361
18.2	基于 HTTP 的 SET 传输	362
18.2.1	HTTP 头	362
18.2.2	HTTP 传输举例	363
18.2.3	错误消息	365
18.3	基于 SMTP 的 SET 传输	365
18.4	基于 TCP 的 SET 传输	367
18.4.1	关闭状态(Closed State)	368
18.4.2	问候状态(Greeting State)	369
18.4.3	认证状态(Authenticating State)	369
18.4.4	打开状态(Open State)	371
18.4.5	关闭状态(Closing State)	372
18.4.6	MIME 封装(MIME - wrapping)	372
18.4.7	传输层控制消息(Transport Layer Control Messages)	373
18.4.8	完整关闭消息(Graceful Close Message)	374
18.4.9	状态消息(Status Messages)	374
18.4.10	回应消息(Echo Messages)	375
18.4.11	非 SET 消息(Non - SET Messages)	376
18.4.12	诊断日志(Diagnostic Log)	377
18.4.13	通讯举例	377
18.4.14	与品牌无关的商家和收单行之间的协定	380

第七部分 电子商务支付系统探讨

第 19 章	SSL 及 SET 分析	383
19.1	网络安全协议	383

19.1.1	OSI 基本参考模型——分层原则和术语	383
19.1.2	Internet TCP/IP 协议组及其与 OSI 结构的关系	384
19.1.3	安全业务的分层配置	386
19.1.4	安全业务管理	389
19.1.5	网络层的安全协议	389
19.1.6	应用层的安全协议	390
19.2	安全套接层协议 SSL	391
19.2.1	SSL 概述	392
19.2.2	SSL 协议分析	394
19.2.3	对协议安全性的分析	396
19.3	SSL 与 SET 协议的比较	396
19.3.1	SET 与 SSL 的比较	397
19.3.2	SSL 和 SET 性能及费用的比较	398

第 20 章 SET 协议扩展及发展趋势

20.1	银行 IC 卡介绍	402
20.1.1	信用卡	403
20.1.2	IC 卡	404
20.1.3	银行 IC 卡特点	405
20.1.4	银行 IC 卡技术和交易特点	406
20.1.5	银行 IC 卡的应用特点	406
20.2	SET 协议对借记卡的扩展思想	407
20.3	SET 协议在线 PIN 扩展	410
20.3.1	商业要求	410
20.3.2	PIN 非对称加密方法	411
20.3.3	对 SET 协议的修改	415
20.3.4	授权请求和响应	416
20.4	通用密文设备 SET 扩展	416
20.4.1	采用通用密码扩展来定义证书和支付扩展的例子	417
20.4.2	扩展使用	419
20.5	SET 协议芯片卡扩展	420
20.5.1	通用芯片卡扩展设计的原则	420
20.5.2	扩展内容	421
20.5.3	非 EMV 数据使用该扩展的原则	421
20.5.4	对 EMV 数据的端到端支持	422
20.5.5	向持卡者应用程序返回数据	422
20.5.6	EMV 芯片卡电子商务规范	423
20.6	商家对非 SET 订购的授权	426
20.7	采用服务器钱包的 SET	428
20.7.1	服务器钱包的工作模式	428
20.7.2	服务器钱包的发布和开始	429
20.7.3	功能	429
20.7.4	认证	430

20.8	SET 算法的发展	430
20.9	经过 SETCo 批准授权的 SET 产品	432
第 21 章	Internet 微支付及其它	437
21.1	数字货币	437
21.2	微支付概述	439
21.2.1	费用因素	440
21.2.2	最小化延迟和计算/存储费用	440
21.2.3	可伸缩性和通用性	441
21.2.4	微支付的安全范围和目的	441
21.2.5	目前微支付的研究情况	442
21.3	IBM 微支付系统	443
21.3.1	支持分散式记账系统的路由协议	444
21.3.2	风险模型和政策发布	444
21.4	IBM 微支付的用户接口和软件结构	445
21.4.1	微支付链接格式	445
21.4.2	动态价格和服务	446
21.5	IBM 微支付协议	446
21.5.1	注册和路由(公钥分发)协议	446
21.5.2	每天的购买者协议	447
21.5.3	购买协议	447
21.5.4	额外消费协议	448
21.5.5	转账和结算协议	448
21.6	电子商务模型语言 ECML	448
21.6.1	HTML 应用举例	449
21.6.2	标记定义	450
21.6.3	SET 与电子商务模型语言 ECML 的结合	453
附录	SET 消息总结	456
附录一	证书请求消息	456
附录二	支附系统消息	457
主要参考文献		460

第一部分

电子商务和支付介绍

本部分介绍电子商务和支付系统的概念，对 SET 协议作总体描述。电子商务的内容包含两个方面，一是电子方式，二是商贸活动。现在人们所探讨的电子商务主要是由 EDI(电子数据交换)和 Internet 来完成的。尤其是随着 Internet 技术的日益成熟，电子商务真正的发展将是建立在 Internet 技术的基础上的。

第 1 章 电子商务和支付系统概述

介绍电子商务的基本知识(特性、发展过程、分类等)，支付系统的概念(支付服务、支付类型、支付模型选择等)，以及电子商务的安全要求和支付协议(安全要求、现有支付协议等)。

第 2 章 SET 协议的总述

介绍 SET 的概念和支付处理流程，包括 SET 标准的组成，SET 支付系统参与者，加密概念，证书发行，购物类型，以及 SET 支付处理的基本步骤。