电子商务安全辞典

Electronic Commerce Security Dictionary

张福德◎编著

Electronic
Commerce
Security
Dictionary

清华大学出版社

电子商务安全辞典

Electronic Commerce Security Dictionary

张福德　编著

清华大学出版社
北　京

内容简介

本书收编的词汇涉及电子商务安全技术、电子商务网络安全技术、电子证书、电子合同、电子数据交换、安全认证技术等。书末附有重要附录。本书具有较丰富的电子商务安全高新技术和高新知识内容，涉及的知识量大，学科多，选材范围极其广泛，适用的对象范围大。

本书是一部电子商务安全技术辞书，较全面系统地记录和整理了电子商务安全的历史与发展史词汇，收集了大量指导目前现实系统与应用的技术，也展示了电子商务安全技术的发展趋势和美好未来。

本书可供电子商务有关研究院、研究生院、各大专院校的研究人员、博士生、硕士生、本科生、大专生和有关导师与教师查阅，也可供IT产业各个公司的管理人员、技术人员以及需要了解电子商务知识和从事电子商务实际工作的读者参考。

版权所有，翻印必究。举报电话：010-62782989　13501256678　13801310933
本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
本书防伪标签采用特殊防伪技术，用户可通过在图案表面涂抹清水，图案消失，水干后图案复现；或将表面膜揭下，放在白纸上用彩笔涂抹，图案在白纸上再现的方法识别真伪。

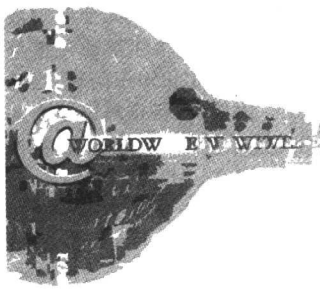
图书在版编目(CIP)数据

电子商务安全辞典/张福德编著．—北京：清华大学出版社，2005.6
ISBN 7-302-10676-2

Ⅰ.电…　Ⅱ.张…　Ⅲ.电子商务-安全技术-词典　Ⅳ.F713.36-61

中国版本图书馆CIP数据核字(2005)第021533号

出 版 者：清华大学出版社　　地　　址：北京清华大学学研大厦
　　http://www.tup.com.cn　　邮　　编：100084
　　社 总 机：010-62770175　　客户服务：010-62776969
责任编辑：徐学军
封面设计：彩奇风
印 刷 者：北京市清华园胶印厂
装 订 者：三河市金元装订厂
发 行 者：新华书店总店北京发行所
开　　本：148×210　印张：11.875　字数：437千字
版　　次：2005年6月第1版　2005年6月第1次印刷
书　　号：ISBN 7-302-10676-2/F·1127
印　　数：1～5000
定　　价：19.80元



编者说明

当今时代为信息时代，当今社会为信息社会。信息既不是能源也不是物质，信息是一个新世界。能源世界遵守能量守恒定律，物质世界遵守物质不灭定律，而信息世界遵守的是无限定律。信息的无限性为人类社会带来了无限的机遇、资源和财富。全世界正在进行信息技术革命，也称为数字化革命。这场革命正在迅速地改变人类的生活方式、生产方式、生存方式、活动方式、学习方式、工作方式、娱乐方式和思维方式。以数字化革命为特点的现代高新技术成果大量涌向社会，使国家与国家、地区与地区、人与人之间的关系发生了重大变化，改变了人们的精神面貌，创建了新的人类社会精神文明和物质文化生活，使全人类进入一个新世界，开辟了人类社会的新纪元。当今社会是电子流行、数字流行、系统流行、信息流行、网络流行和虚拟流行的社会。人类社会已经进入信息化生存、电子化生存、数字化生存、系统化生存、网络化生存和虚拟化生存的时代。

目前，全球大网格(GGG，Grid)正在广泛深入开展。因特网(Internet)的发展分为三大浪潮：第一大浪潮(1960 年至现在)为因特网浪潮。特点是因特网实现了计算机与计算机的联通，服务协议有 telnet://，ftp://，mailto://等。第二大浪潮(1980 年至现在)为万维网浪潮。特点是因特网实现网上内容或万维网网页(Web Home Page)的联通，服务协议为 http://www。第三大浪潮为网格浪潮(1992 年至现在)。网格浪潮是新的因特网大浪潮。特点是因特网实现了网上资源的全面联通，服务协议为 grid://。全球大网格是第三代因特网大浪潮，是实现全球网上所有资源全面联通的因特网技术。

随着因特网的迅速发展，电子商务正在深入人心，大量高新技术、高新技术词汇、高新科学技术知识涌向社会。电子商务的无限前景引起全世界的广泛注意和重视，人们正在利用因特网进行各种各样的商务活动，迅速、广泛、深入发展的电子商务正在动摇和丰富着人们千百年来形成的传统商品交易方式，深刻地改变着人们的传统习惯、思维活动和思想观念。创建电子商务系

统、开展电子商务活动存在各种现代高新技术问题、社会经济问题、金融财政问题、法律税收问题、安全保险可靠问题，还有人们的传统观念和生活习惯等问题。然而，在开展电子商务活动中迫不及待的问题是人才和知识问题，当前我国的电子商务人才奇缺，电子商务知识还未普及。因此，积极培养电子商务人才，系统学习电子商务科学技术知识已是当务之急，这对于广泛开展和推广电子商务活动、创建电子商务系统都具有重大现实意义。

《电子商务安全辞典》是基于我国广泛、深入开展的电子商务科研活动和教学工作编写的，是编著者在撰写《中国电子商务技术》、《电子商务实用技术》、《电子商务与网络银行》、《电子商务安全技术》、《电子商务导论》、《电子商务网络市场》、《网络营销与购物》、《电子商务在企业中的应用》和《电子商务安全认证实用技术》等书的过程中归纳、整理完成的。其早期内容仅用于编著者编著电子商务丛书时附录在电子商务安全方面的书末的《电子商务词解表》，根据广大读者的意见和要求，编著者对其进行了整理、充实、修改和增删，最后完成此书。主要收词范围为电子商务技术、电子商务安全技术、网络银行与金融电子化、电子商务网络技术、电子商务网络市场、国际电子商务贸易和全球电子商务技术等书中的安全技术和安全认证技术。

《电子商务安全辞典》集中了大量的电子商务安全词汇，其特点在于具有较丰富的电子商务安全的高新技术和高新知识内容、知识面广，是涉及许多学科的综合学科，适用的对象范围很广。《电子商务安全辞典》较全面系统地记录和整理了电子商务安全方面的历史与发展史的词汇，收集了大量指导目前现实系统与应用的技术，也展示了电子商务的发展趋势和美好未来，可供电子商务有关研究院、研究生院、各大专院校的研究人员、博士生、硕士生、本科生、大专生和有关导师与教师查阅，也可供广大 IT 产业各个公司的管理人员、各种技术人员以及需要了解电子商务知识和从事电子商务实际工作的读者参考。

编著者于 1990 年编写《中国金融电子化全书》时研究了电子数据交换(EDI)，从 1994 年开始潜心研究电子商务技术、虚拟现实技术、网络银行和手机银行等技术，专心编写《电子商务》丛书。出版一本《电子商务安全辞典》是编著者的夙愿。编著者在对外经济贸易大学、中国社会科学院研究生院从事电子商务教学过程中，不断收集、研究和积累电子商务有关词汇，进行了全面系统的整理、充实和修改，完成本书。编著者深知，编写《电子商务安全辞典》是一项浩大的工程，电子商务技术是一门涉及范围极广的高新科学技术，遇到有关的新问题也极多，大量的新词汇还在不断地涌现。因此，本辞典虽称全面，也仅是沧海一粟。因编著者水平有限，时间仓促，书中难免挂一漏万，择轻忘重，恳请广大读者批评指正，多提建议和要求，以便再版时补充修正。

参加本书编写的还有：邓淑娜、方国兴、郑伟、张福春、耿雪霏、邹红伟、刘

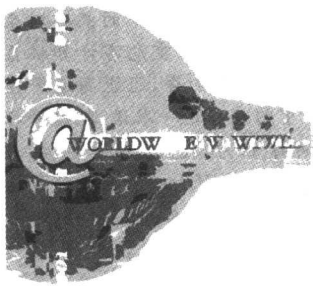
此为试读，需要完整PDF请访问：www.ertongbook.com

亚辉、温延春、许明、高宏志、宋学明、李跃臣、王唯力、孙波、陈志萍、魏岳鹏、陈宝林、杨虹、杨范、张庆欢、黄家琳、张新颖、张南英、方争群、陈玉原、陈玉莲、陈玉春、陈玉娟、刘曼、张福恩、史大清、史宇、王浩、张涛、孙立元、孙立人、姜美。

本书的出版得到清华大学出版社的大力支持，在此表示衷心的感谢。如本书能对我国乃至世界电子商务事业有所贡献，对广大读者、科研人员和高等院校师生有所裨益，编著者将感到无限欣慰。

对外经济贸易大学教授　张福德

2005 年 1 月 6 日　北京



凡 例

1. 查阅说明

本辞典主要收词范围为电子商务安全技术、电子商务网络安全技术、电子认证证书、电子合同、电子数据交换、安全认证技术等。本辞典为汉—英辞典。

2. 汉—英部分

本辞典绝大多数词汇的结构为：(1)一个或者多个汉语词汇；(2)英文缩写；(3)英文全称和其他多种英文缩写；(4)汉语释义。

3. 举例

例(1)

病毒(计算机病毒，计算机网络病毒，因特网病毒)

CV(Computer Virus)

病毒(Virus)一词来源于生物学。在生物学中，病毒是能够侵入生物体并给生物体带来疾病和造成毒害的一种微生物。这种微生物在侵袭并危害生物体的过程中具有下列特点：(1)借某种媒介侵入生物体内，以该生物体作为宿主潜伏下来并进行繁殖。(2)病毒能在生物体间进行传染，而且使受传染的生物体成为新的传染源。(3)凡是被病毒传染的生物体都有某些正常生理机能被损害等受毒害的症状。自从1988年以来，在计算机领域内有这种越来越

多的程序，它们对计算机系统的危害以及危害的方式与生物界中的病毒对生物体的危害以及危害的方式有着完全类似的特征。这种严重危害计算机系统的程序很像微生物学中的病毒，不仅在计算机系统中生存，还能高速繁殖和传播，危害性极大。于是人们便借用了生物学中的病毒这一术语，把这种程序叫做“病毒程序”或者简称为“病毒”。“病毒程序”包括计算机病毒(Computer Virus)、计算机网络病毒(Computer Network Virus)和因特网病毒(Internet Virus)。计算机病毒是一种能够进行自我繁殖或自我复制的程序，可以通过多种方式被植入计算机中，通过因特网植入病毒更加容易，已引起人们高度的重视。病毒运行后可能损坏文件、使系统瘫痪，造成各种难以预料的后果。由于在网络环境下，计算机病毒具有不可估量的威胁性和破坏力，因此，加强对计算机病毒、计算机网络病毒和因特网病毒的防范在计算机系统安全和网络安全性建设中具有极其重要的现实意义。计算机病毒与微生物病毒类似，具有侵入、繁殖、感染和毒害等迅速广泛严重的破坏作用。狭义的病毒是隐藏在其他程序中的一段代码，其具有潜伏能力、自我繁殖能力和被激活产生破坏的能力。广义的病毒还包括逻辑炸弹、时间炸弹、蠕虫、种子程序、细菌程序和兔子程序等。逻辑炸弹是在程序中设置了一些引爆条件，当这些条件满足时，立即发生逻辑爆炸，程序将会做与原来功能不一样的事。时间炸弹是一种在定期、定时、定数等引爆条件下能立即执行破坏性指令的程序，因此，它们通常是在满足特定的时间和数目时发作的。蠕虫是一种可以在网上不同主机之间迅速进行广泛传播，而不需修改目标主机上其他程序的一类程序。它大量进行自我繁殖而并不一定具有潜伏能力和激活能力，它一旦进入系统就能迅速广泛繁殖，最终导致整个系统瘫痪。种子、细菌和兔子程序都是自我繁殖能力极强的程序，是一类疯狂复制自己，以消耗系统资源的破坏性程序。这种程序不断地自我繁殖或复制自己，直到没有足够的磁盘空间或内存空间可以容纳其下一代繁殖为止。

其中，“病毒(计算机病毒，计算机网络病毒，因特网病毒)”为多个汉字词汇；“CV”为相应的英文缩写；“Computer Virus”为其相应的英文全称及其他缩写形式。汉语释义部分为：“病毒(Virus)一词来源于生物学。在生物学中，病毒是能够侵入生物体并给生物体带来疾病和造成毒害的一种微生物……”

通过英文索引可以查到：CV(Computer Virus)。通过汉语拼音顺序的中文索引可以查到：病毒(计算机病毒，计算机网络病毒，因特网病毒)。

例(2)

认证证书申请程序

CRP(Certificate Required Program)

所有想获得证书者(不包含签发管理中心)必须在一个完整时间内，完成

下列认证证书申请的一般程序:(1)产生一组密钥对并向受理的签发管理中心证明此密钥对为有效的密钥对。(2)保护此密钥对的私密密钥,以避免其遭到破坏或盗用。(3)确定一个可供识别的名称。(4)向合适的签发管理中心提出证书申请(与用户合同),其中包含此密钥对的公开密钥。

其中,"认证证书申请程序"为汉字词汇;"CRP"为相应的英文缩写;"Certificate Required Program"为其相应的英文全称。汉语释义部分为:"所有想获得证书者(不包含签发管理中心)必须在一个完整时间内,完成下列认证证书申请的一般程序:(1)产生一组密钥对并向受理的签发管理中心证明此密钥对为有效的密钥对。(2)保护此密钥对的私密密钥,以避免其遭到破坏或盗用。(3)确定一个可供识别的名称。(4)向合适的签发管理中心提出证书申请(与用户合同),其中包含此密钥对的公开密钥。

通过英文索引中可以查到 CRP(Certificate Required Program),通过汉语拼音顺序的中文索引可以查到:认证证书申请程序。

例(3)

施工索赔(索赔,施工理赔,理赔)

CC(Construction Claim;Settlement of Claim,SOC)

在国际工程承包中,由于业主或其他方面的原因,使承包商在施工过程中付出了额外的费用,承包商根据有关规定,通过合法的途径和程序,要求业主或其他方面偿还他的费用损失的行为称为"施工索赔",简称为"索赔"。而业主或其他有关方面对承包商提出的要求进行处理,称为"施工理赔",简称为"理赔"……

其中,"施工索赔(索赔,施工理赔,理赔)"为多个汉字词汇;"CC(Construction Claim,Settlement of Claim,SOC)"为相应的英文缩写和全称;在"国际承包中……"为汉语释义部分。

4. 在英文索引和中文索引中,每个词后面的括号内的数字为该词所在的页码数,例如:

(1) CRP(Certificate Required Program)(195),表明这个词在第 195 页;

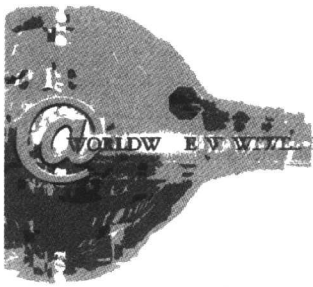
(2) 认证证书申请程序(195),表明这个词在第 195 页;

(3) CV(Computer Virus)(30),表明这个词在第 30 页;

(4) 病毒(计算机病毒,计算机网络病毒,因特网病毒)(30),表明这个词在第 30 页。依此类推。

5. 书末有附录，供读者参考

附录1：CXO；附录2：E(Electronic)——电子化；附录3：X to X；附录4：计算机病毒活动日期与时间；附录5：电子签名法；附录6：编著者的主要有关论文和书。



目录

此为试读,需要完整PDF请访问: www.ertongbook.com

阿米巴磁盘病毒(变形虫磁盘病毒,阿米巴病毒,变形虫病毒)

Amoeba

发作时,盖写硬盘起始的一些磁道,伴随有闪烁的信息,并在磁盘被盖写的扇区中留下一句名言。

阿米利亚病毒(Amillia 病毒)

AV(Amillia Virus)

是一种定时发作的病毒,在 2 月 2 日发作。

爱虫病毒(我爱你病毒)

I love you

2000 年 5 月 4 日从菲律宾首都出现了"爱虫"病毒(I love you 病毒),它横扫因特网,疯狂袭击全球计算机网络、政府、商家企业和个人,在一天之内就产生了几十个变种,在短短的几天之内,仅仅"爱虫"病毒自己就创下了造成 65 亿美元损失的空前记录。

安全保密(安全性/保密性)

S/C(Secrecy/Confidentiality)

主要是指防止对信息的各种非授权访问。这是对信息和数据的安全要求,也是最重要的要求。

安全标签(敏感性安全标签)

SL(Sensitivity Label)

主要是指具有敏感性的安全标签,保证敏感信息的安全。

安全策略

SP(Secure Policy)

是指以 PPDR 安全模型为核心的策略,所有的安全防护、检测、响应都是依据安全策略实施的,企业安全策略为安全管理提供管理方向和支持手段。策略体系的建立包括安全策略的制定、评估、执行等。制定可行的安全策略取决于对网络信息系统的了解程度。

安全超文本传输协议(SHTTP 协议)

SHTTP(S-HTTP,S-http,Secure HTTP,Secure Hyper Text Transport Protocol)

安全超文本传输协议(SHTTP 协议)依靠密钥的加密,保证万维网站点间的交换信息传输的安全性。SHTTP 协议是扩充了超文本传输协议的安全特性、增加了报文的安全性而产生的,它是基于 SSL 技术的协议。SHTTP 协议面向因特网的应用提供了完整性、可鉴别性、不可抵赖性及机密性等安全措施。目前,SHTTP 协议正由因特网工程任务组起草 RFC 草案。通常,SHTTP 协议只用于万维网业务,保障万维网站点间的交易信息传输的安全性。安全超文本传输协议是利用密钥对文本进行加密,依靠密钥的加密,保证万维网站点之间进行交换信息传输的安全性。

安全措施

SM(Security Measures)

是指任何使用或信任由认证中心公共认证服务所签发的认证证书及相关信息者,应对该信息采取合理的安全措施,以便于他方认证该信息,并在必要时支持信息保密功能。

安全第一软件(绝对安全软件,SWFS 软件)

SWFS(Secure Way First Secure)

安全第一软件也称为绝对安全软件或 SWFS 软件,它通过提供防病毒、存取控制、传输容量控制、防侵入、数字签名、防火墙以及其他已实现的安全服务,可以保证商家企业(公司)能够在网络上进行安全的网络活动。

安全电子交易协议(安全电子交易标准,安全电子交易规范,电子商务安全交易协议,SET 协议)

SET(Secure Electronic Transaction)

是为了在开放的网络上提供一种进行安全的支付卡交易的方法而发布的开放工业标准,其特点是交易与信用卡绑定,是一种允许在万维网上进行安全信用卡支付的标准。随着因特网、万维网技术的高速发展,电子商务得到广泛应用。由于因特网本身的开放性,使网上交易面临种种危险,网上欺骗、窃听、非法入侵都在威胁着电子商务。因此,提出了相应的安全控制要求。要求网络能提供一种端到端的安全解决方案,包括加密机制、签名机制、身份认证等。在这样的背景下,安全电子交易协议 SET 便应运而生。SET 标准被公认为全球网际网络的标准,其交易形态将成为未来电子商务的技术规范。1. 安全电子交易协议开发过程。SET 由 Visa 和 Master Card 首先提出,并得到 IBM 等国际大公司的支持。1995 年,信用卡国际组织、资信业者及网络安全专业团体等开始组成策略联盟,共同研究开发电子商务安全电子交易协议。1996 年 2 月 1 日,Master Card 和 Visa 国际信用卡组织与技术合作伙伴

GTE、Netscape、IBM、Terisa Systems、Verisign、Microsoft、SAIC 和 Terisa 等一批跨国公司共同开发了安全电子交易规范(SET)。1996 年 6 月发布了安全电子交易协议(SET 协议)的正式公告,涵盖了信用卡在电子商务交易中的交易协定、信息保密、资料完整、数字认证和数字签名等。2. 安全电子交易协议是在开放网络环境中的卡支付安全协议,它采用公开密钥密码体制(PKI,也称为公开密钥基础设施)和 X.509 电子认证证书标准,通过相应软件、电子认证证书、数字签名和加密技术能在电子交易环节上提供更大的信任度、更完整的交易信息、更高的安全性和更少受欺诈的可能性。(1)安全电子交易协议用以支持企业对消费者(B to C)这种类型的电子商务模式,即消费者持卡在网上购物与交易的模式。(2)电子安全交易协议技术。SET 协议使用的主要加密技术有:①密钥系统(也称为对称密码系统)。②公钥系统(也称为非对称密码系统)。③数字签名技术。④哈希算法。⑤双重签名等技术。在电子安全交易协议(SET)中,使用 SHA-1 哈希函数、DES 算法和 RSA 算法提供数据加密、数字签名、数字信封等功能,对交易信息在网上传输提供了安全保证。运用 DES 算法与 RSA 算法,以便确保网上传输信息的秘密性。认证的交换验证配合数字签名,以便以确认交易双方的身份,进一步提供不可否认的功能。以数字信封、双重签名确保信息隐私性与关联性。使用 SHA-1 哈希函数与 RSA 密码算法构成数字签名,以便确保信息的完整性,防止篡改和伪造。(3)安全电子交易协议的安全电子交易基本流程:①客户资料要通过商家到达银行,但商家不能阅读这些资料,所以 SET 解决了客户资料的安全性问题。②SET 协议解决了网上交易存在的客户与银行之间、客户与商家之间、商家与银行之间的多方认证问题。③由于整个交易过程是建立在 Intranet、Extranet 和 Internet 的网络基础上的,因此 SET 协议保证了网上交易的实时性和安全性。安全电子交易协议涵盖了信用卡在电子商务交易中的交易协定、信息保密、资料完整、数字认证和数字签名等。这一标准被公认为全球网际网络的标准,其交易形态将成为未来电子商务安全的规范。(4)电子商务安全交易协议(SET)的文件主要由三个文件组成:①SET 业务的描述。②SET 程序员指南。③SET 协议的描述。安全电子交易协议(SET)是重要的电子商务安全电子交易协议。(5)SET 协议规定了交易各方进行安全交易的工作流程,信息的传送都使用 SET 协议以保证其安全性。电子钱包是 SET 在用户端的实现,电子商家是 SET 在商家的实现,支付网关是 SET 在金融方的实现。具体的交易过程如下:①用户使用浏览器在商家的主页上查看商品目录和商品介绍。②用户选择要购买的商品后,主页出示订单让用户确认。订单内容包括项目列表、单价、总价、送货费等。③用户确定后,发送给商家定单信息及支付信息,前者供商家确认,后者则由商家转发支付网关进行转账处理。订单信息及支付信息都要用户进行数字签名。④商家接收订单后,将确认信息及用户

的支付信息发送给支付网关。⑤支付网关验证用户的支付信息。确认后联系商家的收单银行和用户的开户银行进行转账。转账成功后向商家返回信息。⑥商家发送订单确认信息给用户，用户端软件记录交易日期，以备将来查询。⑦商家给用户送货，交易完成。在上述交易过程中，涉及信息加密技术、数字签名技术、数字摘要技术和数字认证证书、认证管理等各种技术。

安全电子交易协议的认证证书格式(SET 认证证书格式，SET 认证格式)
SETCA(Secure Electronic Transaction CA，SET Certificate Authority)

认证证书格式比较特殊，虽然它也遵循 X.509 标准，但主要是由 Visa 和 Master Card 开发并按信用卡支付方式来定义的。银行的支付业务不仅仅是卡支付业务，而安全电子交易协议支付方式和认证结构仅适应于卡支付，对其他支付方式还是有限制的。

安全电子邮件协议(电子邮件扩充标准格式，安全的多功能因特网电子邮件扩充协议，SMIME 协议，安全电子邮件管理协议，S/MIME 协议)
SMIME(S/MIME，Secure/Multipurpose Internet Mail Extensions)

是在因特网上用来发送安全电子邮件的协议。SMIME 协议是一种在因特网安全电子邮件管理环境中采用的加密报文语法，是对电子邮件安全性进行处理的规则，主要用于电子邮件的收发业务或者电子邮件的应用业务，也可以用于万维网业务。SMIME 协议是在 RFC1521 所描述的多功能因特网电子邮件扩充报文基础上添加数字签名和加密技术的一种协议。SMIME 协议是正式的因特网电子邮件扩充标准格式，但它未提供任何的安全服务功能。SMIME 协议的目的是在安全电子邮件管理协议上定义安全服务措施的实施方式。为了使用安全电子邮件协议，在客户端必须使用支持 S/MIME 协议的电子邮件程序，例如 IE Outlook Express 和 Netscape Messenger。SMIME 协议已成为产业界广泛认可的协议，例如微软公司、Netscape 公司、Novel 公司、Lotus 公司等都支持 SMIME 协议。

安全防护(安全保护)
SP(Secure Protection)

通常是指通过采用一些传统的静态安全技术及安全方法来实现的安全防护，主要有操作系统访问控制、防火墙、加密和认证等安全保护方法。

安全服务(认证证书安全服务，SS 服务)
SS(Security Services)

主要是指认证证书安全服务，也称为数字认证证书安全服务(Certificate Security Services)。认证中心的公共认证服务支持各种安全机制，以保护通信及信息等相关资源。但是单凭认证过程并不能建立这种安全机制，而是在认证中心公共认证服务的架构下，其他通信者能使用这种信息安全服务。这

套架构使用数字签名及认证，保护在开放网络中安全地进行的通信及电子商务，并监测安全服务是否达到预期效果。

安全服务方法论(PADIMEE 方法论，安全服务的策略—评估—设计—执行—管理—紧急响应—教育方法论)

PADIMEE(Policy, Assessment, Design, Implementation, Management, Emergency Response, Education)

是基于信息安全国际标准(BS7799/ISO17799/SSE-CMM)的方法论。其中的 PADIMEE 方法内容如下：(1)策略(Policy)。(2)评估(Assessment)。(3)设计(Design)。(4)执行(Implementation)。(5)管理(Management)。(6)紧急响应(Emergency Response)。(7)教育(Education)。安氏公司根据安全服务方法论，针对客户对信息安全的实际需求与资源状况，推出信息安全全面解决方案。由安全管理咨询、安全系统集成服务、安全客户支持、安全培训等一系列服务组成，包括构建一个安全无忧的信息安全环境所涉及的各个环节，是全面保证信息系统安全的解决方案。其目标是帮助用户建设完整可靠的信息安全体系，从用户对安全的需求出发，为用户提供全面的信息安全解决方案。

安全服务工具 Praesidium(电子商务安全产品解决方案)

Praesidium(HP Praesidium)

是指惠普公司开发的电子商务安全产品解决方案。Praesidium 是惠普公司 E-security 安全性解决方案的产物，主要由外部虚拟专用网、数据加密、防火墙、身份认证和安全操作系统等不同技术构成，从数据传输、企业安全和应用等方面为电子商务安全服务。安全服务工具具有很强的万维网(Web)认证功能，结合第三方或用户自己的目录服务，这一安全服务系统作为一个安全应用开发组件为授权服务器提供了用户认证功能。具有灵活和易于管理的特点。安全服务工具利用 DES 保密编码模块，允许用户安全地进行登录和数据传输。安全服务组件虽然提供一次性认证登录软件的组件(DCE)级的认证，但它并不需要一次性认证登录软件的组件。安全服务组件是安全应用服务器的安全服务解决方案的一部分。安全服务工具的安全保障产品都是基于业界的标准设计的，可支持多种硬件平台，并且可以工作在多种供应商的计算环境中。由于注意了对安全问题解决方案的安全、集中、方便的管理上的要求，因此，正在进一步加强操作管理平台(Open View)的安全性能。实际上，操作管理平台是安全服务工具、安全产品、安全解决方案和安全管理的平台。

安全工作区

Zoning

在 SAN 标准环境中这是一个安全的工作区，具有光纤通道规范，用它将

此为试读，需要完整PDF请访问：www.ertongbook.com