

国家骨干高职院校建设成果 | 电子商务专业工作过程导向型教材 |

电子商务法律法规

刘志慧 主编 / 高慧云 戚会庆 副主编



清华大学出版社

| 国家骨干高职院校建设成果 | 电子商务专业工作过程导向型教材 |

电子商务法律法规

刘志慧 主编 / 高慧云 戚会庆 副主编

清华大学出版社
北京

内 容 简 介

本书以《国家教育事业第十二个五年规划》文件为指导,紧扣高职高专教育培养应用型人才目标要求,以专业职业能力培养为主线,从全新的视角,本着理论和实际密切结合的原则,阐述了电子商务法涉及的基本问题,包括电子签名和电子认证、电子合同、电子支付等法律规范;着重探讨了有关电子商务市场法制环境的问题,包括网络知识产权保护、个人隐私权、虚拟市场规制、电子商务税收、电子证据和司法管辖等;对于网络游戏等最新的电子商务法律难题,以及电子商务法律新问题也作了介绍。

本书可作为高职高专、成人高校电子商务专业教学用书和非电子商务专业(如工商管理、信息管理、计算机等)的教学用书,也可供五年制高职学生使用,还可以作为广大电子商务从业人士的有益参考书。

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。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

电子商务法律法规/刘志慧主编. —北京:清华大学出版社,2015
国家骨干高职院校建设成果 电子商务专业工作过程导向型教材
ISBN 978-7-302-37075-8

I. ①电… II. ①刘… III. ①电子商务—法规—中国—高等职业教育—教材
IV. ①D922.294

中国版本图书馆CIP数据核字(2014)第146066号

责任编辑:左卫霞

封面设计:傅瑞学

责任校对:李梅

责任印制:何芊

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦A座 邮 编:100084

社总机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

课 件 下 载: <http://www.tup.com.cn>, 010-62795764

印 装 者:三河市金元印装有限公司

经 销:全国新华书店

开 本:185mm×260mm 印 张:15.5 字 数:351千字

版 次:2015年1月第1版 印 次:2015年1月第1次印刷

印 数:1~3000

定 价:29.50元

高等职业教育作为一种职业教育类别,与高等本科教育的根本区别在于它是以服务为宗旨,以就业为导向的教育,因此衡量高等职业教育的唯一标准是学生的就业和创业能力。整合教育资源、改进教学方式是当前职业教育改革创新着眼点和着力点,其中最关键的是推动学校与企业联合办学,实行校企合作、工学结合。高职高专的教材要体现高职高专的教改成果,要符合高职高专的发展动态和特点,需要企业与学校共同合作设计,要结合企业的工作内容来设计学习内容,要根据学生的心理特点和接受能力来编排教材体例,激发学生的阅读兴趣,培养学生的实践能力和综合素质。

作为一本高等职业教育的教材,本书在体例设计上依据电子商务类高职高专未来的工作岗位要求进行设计,结合与实际操作相关的理论知识;在内容安排上以通过企业案例和学生模拟将相关的法学知识融入教学中,让学生在学中思,思中进行理论的升华。

本书具有以下特点。

(1) 全书以实际工作情境贯穿始终。本书以电子商务管理类人员的职业为视角,以来自工作中的案例为主线设计教材内容,注重理论和实践的融合。通过从实际工作中搜集案例并精心设计,将理论融入案例中,学生可以带着案例逐步学习理论,分析案例后逐步学习理论,最终达到理论体系的再造和升华。这种从具体到一般的学习方法符合人的认知规律,符合高职学生的心理接受能力。

(2) 本书每章正文以情境导入开始,选取在实际生活和工作中的典型情境,统领章节内容体系。文中每章采用一家公司企业在实际业务往来中可能遇到的问题,采用以案说法的形式编排理论内容,其间还穿插学前思考、小贴士、同步案例等,体现教师主导作用和学生主体作用的和谐统一,拓展学生的思维领域,锻炼学生分析与解决问题的能力,强化师生之间、学生之间的互动交流。实现了知识与趣味、理论与实践、法律与案例的有机结合。

(3) 注重教材的深度和培养学生的可持续发展能力。在重视高职高专教育实践性的同时,本书也没有忽视高职高专的理论基础和案例的深度问题,吸纳了截至2014年5月1日的最新电子商务方面的法律法规信息,同时也加入了目前存在争议的问题以及国际通行的做法,从而使理论深度和知识面得到加强。

(4) 宽泛的内容体系。为扩展本书使用的广泛性,本书在内容的选取上更加宽泛,读者在使用本书时,可根据自己的职业特点确定学习内容,有所取舍。

本书编写人员既包括有多年电子商务法教学经验的老师,又包括有丰富法律从业经验的电子商务师。具体分工如下:北京信息职业技术学院教师、北京市京都律师事务所兼职执业律师高慧云负责编写第1、6、7、8章;北京信息职业技术学院教师刘志慧负责编写第2、4、5章;北京江南天安科技有限公司高级项目管理师戚会庆负责编写第3章。

本书由刘志慧对全书篇章进行结构设计,高慧云负责对教材进行修改、整理,戚会庆负责对实践性案例进行审查。

当然,本书仅仅是在高职高专教学改革过程中向前走了一小步,还需要我们不断努力,以学生为中心,真正培养学生的综合能力,编写出更受读者欢迎的教材。真诚地希望读者能够提出宝贵的建议和意见,并发送至电子邮箱 liuzh@bitc.edu.cn。

编者

2014年8月

本书导语

张莹是一名电子商务专业的学生,非常喜欢网络游戏,对网络游戏公司也非常好奇,因此在大三实习期间,她选择了一家网络游戏公司——北京慧通网络发展有限公司实习。该公司是一家网络游戏运营商,是通过电子商务进行网上运营的网络游戏公司,其经营模式为通过自主开发或取得其他游戏开发企业授权运营网络游戏,同时与漫画、音乐、影视等各种数字娱乐领域的公司合作,以出售游戏时间、游戏道具或相关服务为用户提供增值服务和游戏内置广告(IGA)获得收入。玩家可以选择按时间计费或通过购买道具计费两种方式。按时间计费的玩家可以通过时间累积免费获得相应道具。付费渠道主要是购买点卡和通过网络商付费。

在张莹的后续工作中,遇到了很多相关法律问题,让我们一起帮助张莹解决吧。

第一章 电子签名与认证法律制度	1
第一节 电子签名概述	2
一、电子签名的概念	3
二、电子签名的分类	5
三、数字签名	6
第二节 电子签名的适用范围和法律效力	10
一、电子签名的适用范围	10
二、电子签名的法律效力	11
第三节 电子签名人、电子签名依赖方的义务和责任	14
一、电子签名人的义务和责任	14
二、电子签名依赖方的义务和责任	16
第四节 电子认证机构	17
一、认证机构的概念	17
二、电子认证机构的设立	17
三、电子认证机构提供的认证服务的内容	18
四、电子认证服务的更新、暂停和撤销	19
第五节 电子认证中各方的法律关系	19
一、认证机构和证书持有人之间的权利和义务	19
二、认证机构和证书信赖人之间的权利和义务	22
三、认证机构的法律责任	23
小结	26
职业能力检测	26
第二章 电子合同法律制度	28
第一节 电子合同概述	29
一、电子合同立法的发展	29
二、电子合同的概念	30
三、电子合同的特征	31
四、数据电文的证据性	32
五、电子错误责任的承担	35
第二节 电子合同的订立	36
一、电子合同的主体	36

二、电子合同的要约、要约邀请与承诺	40
三、在线交易中的要约、要约邀请与承诺的界定	43
四、电子要约和承诺的撤回	45
五、电子要约的撤销	45
六、电子要约的生效	46
七、要约和承诺的收讫确认	47
第三节 电子合同的成立	50
一、电子合同的成立时间	50
二、电子合同成立的地点	51
第四节 电子合同的履行	53
一、电子合同履行原则	54
二、电子合同当事人的权利和义务	54
第五节 有关电子格式合同的法律问题	60
一、电子格式合同问题的产生	60
二、国外的相关判例及立法	62
三、我国相关的法律规定	67
小结	68
职业能力检测	68
第三章 电子支付法律制度	69
第一节 电子支付概述	70
一、传统支付方式及法律规定	70
二、电子支付概述	72
第二节 电子支付的工具	75
一、电子现金	75
二、电子支票	77
三、电子信用卡	78
四、网上银行	81
第三节 电子支付当事人概述	82
一、电子支付的当事人	82
二、电子支付当事人的法律关系	82
三、电子支付当事人的权利义务	83
第四节 电子支付的法律问题	85
一、国外电子支付立法情况	85
二、我国电子支付立法情况	87
三、电子支付面临的法律问题	87
四、电子支付立法展望	91
第五节 电子发票概述	93

一、电子发票	94
二、纸质发票与电子发票的对比	95
三、国际上电子发票的使用情况	96
四、我国电子发票的使用情况	97
小结	98
职业能力检测	99
第四章 虚拟财产的权属	100
第一节 虚拟财产的范围和主体	101
一、虚拟财产的概念和特征	102
二、国外目前立法现状	103
三、我国虚拟财产保护现状	105
第二节 虚拟财产纠纷的责任	106
一、虚拟财产纠纷	106
二、虚拟财产的物权法责任	108
三、虚拟财产的合同法责任	112
四、虚拟财产的侵权法责任	114
五、虚拟财产的继承法责任	118
小结	119
职业能力检测	120
第五章 电子商务与消费者权益保护法	121
第一节 消费者权益保护法概述	122
一、消费者权益保护法的概念和特征	122
二、消费者权益保护法的主要内容	123
第二节 在线交易消费者及保护	126
一、在线交易消费者	126
二、网络环境消费者保护的特殊性	128
三、经合组织消费者保护的主要框架	128
四、现行消费者权益保护法对在线交易消费者的保护	131
第三节 经营者的义务	138
一、网络服务经营者的基本义务	138
二、提供商品信息的义务	139
三、商品质量保障及售后服务义务	140
四、不得有不当免责的义务	141
第四节 在线交易消费者隐私保护	142
一、网络环境下的隐私权保护	142
二、个人信息隐私权保护概述	144

三、各国及地区保护消费者隐私权的法律对策	147
小结	149
职业能力检测	150
第六章 电子商务与知识产权法	151
第一节 著作权的保护	152
一、网络著作权概述	152
二、网络著作权立法状况	153
三、网络著作权主要涉及的法律问题	154
四、网络著作权的限制	164
第二节 域名的保护	167
一、域名概述	167
二、域名的管理机构及注册	169
三、域名纠纷及其法律保护	170
四、域名争议解决机制	177
五、通用网址及其法律保护	179
小结	181
职业能力检测	181
第七章 电子商务与税收法律制度	183
第一节 现行税法概述	184
一、税收和税法	184
二、税收管辖权	187
第二节 电子商务对现行税收制度的影响	188
一、电子商务对税法基本要素的影响	189
二、电子商务对现行各税种的影响	190
三、电子商务征收新税问题	193
四、电子商务过程的税收征管问题	193
第三节 我国电子商务税收法律制度	197
一、增值税	197
二、营业税	201
三、印花税	202
小结	203
职业能力检测	203
第八章 电子证据与电子商务争议	204
第一节 电子商务争议解决方式	205
一、在线争议解决方式的种类和优点	205

二、在线协商	205
三、在线调解	206
四、在线仲裁	208
五、在线诉讼	213
第二节 电子商务纠纷的管辖	213
一、法院的管辖权	214
二、传统纠纷管辖权的确定	214
三、网络纠纷管辖权遇到的法律障碍	216
四、中国网络纠纷管辖权的确定	218
五、国际公约关于网络纠纷管辖权的规定	219
六、管辖权法律风险的防范	220
第三节 电子商务诉讼中的电子证据运用	222
一、请求国家机构给予协助的措施(公权力救济措施)	223
二、电子证据收集技术和方法	226
三、电子证据在司法实践中的应用	230
小结	231
职业能力检测	231
附录 本书引用的主要法律、法规	233
参考文献	235

第

章

电子签名与认证法律制度

知识目标

1. 熟悉电子签名的概念。
2. 了解电子签名的种类。
3. 掌握电子签名的效力。
4. 熟悉电子签名的程序。
5. 熟悉电子认证机构。

能力目标

1. 通过运用正确电子签名的过程,保护企业的正当权益。
2. 通过运用所学电子签名的知识,避免企业与企业、企业与用户之间产生纠纷。

情境导入

张莹在北京慧通网络发展有限公司工作初期,被安排做网络游戏开发工作中的联络沟通工作,以保证每个员工工作有序。每个游戏项目的开发需要一系列工序,包括游戏策划、美工、动画、音乐创作、测试支持等流程。每个流程结束均要求负责人签字。该游戏公司采用了OA办公电子签名系统,通过电子签名来确认工序的完成。在其工作过程中,张莹遇到如下问题。

1. 美工组的组长因为生病,由其组员李娜代替其进行签名。
2. 由于采用的是秘钥方式进行签名的传递,音乐创作的秘钥被其他公司盗取了,并且新创作的动画配乐被拿掉了。
3. 由于公司的会计部门处于交接中,会计部门未能按时交电费,导致供电局突然停

止供电,公司动画部正在制作的动画未能保存造成客观的经济损失。公司与供电局理论,认为不能随便断电,但是供电局答复曾经给公司的财务部门多次发过邮件催缴,但是无人理会,故此采取断电方式。

如果你是张莹,遇到上述问题应当如何解决?并说明理由。

网络是一个虚拟的世界,交易各方信息的交流是通过互联网进行的,电子商务中交易各方可能从来没有见过面,从而使得各方无法确定对方的身份,因此必然使人们对交易的安全感到担心,而且由于网络的开放性,人们还担心数据在传输过程中被篡改。所以如何鉴定各方的身份,保证数据传输的真实性,以保证交易的安全,是电子商务中一个非常重要的问题。为了解决这一问题,人们发明了电子签名技术,并建立了具有第三方地位的中立的认证机构,以确保交易各方身份的真实性和数据传输的可靠性。但是,电子签名和以网络技术为基础的认证机构,是从来没有过的新鲜事物,现行法律很难直接适用。因此如何对电子签名和认证机构进行调整,是必须明确的法律问题。

第一节 电子签名概述

电子签名是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。通俗地说,电子签名就是通过密码技术对电子文档的电子形式的签名,并非是书面签名的数字图像化,它类似于手写签名或印章,也可以说它就是电子印章。



小贴士

电子签名和纸质签名有类似的效力。电子签名是电子商务安全的重要保障手段。特别是在联合国《电子商务示范法》颁布之后,国际组织及一些发达国家,都将其立法的焦点从书面问题转向了电子签名。这是一个如何使交易者的身份与其电子记录相联系的技术性问题,同时又是一个全新的法律问题^①。

传统上的签名,是指在书面材料上写上执笔者名字。美国《统一商法典》对“签名”的定义为:包括当事人意图认证一份书面材料所作的或所使用的任何符号。签名的决定性因素是签署者当时证明书面文件的意图。而认证可能是打印的、盖章的,或书写的,还可能仅仅是简写或指模,甚至在某些特定的案件里,可将信笺印刷的字迹作为签名。

电子签名并非是书面签名的数字图像化。它其实是一种电子代码,利用它,收件人便能在网上轻松验证发件人的身份和签名。它还能验证出文件的原文在传输过程中有无变动。如果有人想通过网络把一份重要文件发送给外地的人,收件人和发件人都需要首先向一个许可证授权机构 CA(GlobalSign)申请一份电子许可证。这份加密的证书包括了

^① 张楚.《电子商务法初论》[M].北京:中国政法大学出版社,2000.

申请者在网上的公共钥匙即“公共电脑密码”,用于文件验证。

但是,数据电文不带有手写的签字,而且也不在纸上。电子形式的信息很容易在不被发现的情况下被截获和篡改,所以利用数据电文欺诈的潜在可能性很大。因此,数据电文要被广泛使用,必须有这样的技术手段,即在电子环境下能够借助于这些手段履行被认定为手写签字所独具的某些或全部功能。这类技术可统称为“电子签名”。电子签名与一般将手写签字扫描到计算机存为文件截然不同,后者如通过电子邮件方式传送给他人,收件人可以轻易地复制该签名而达到伪造文件或欺诈的目的;前者经过加密处理,他人无法轻易地复制该签名或更改文件内容,安全性相当高。^①

一、电子签名的概念

对于电子签名的概念有几种不同的认识,各种认识都有其一定的合理性。

(一) 广义的电子签名

广义的电子签名,是指包括各种电子手段在内的电子签名。联合国贸易法委员会《电子签字示范法》^②第二条第一款规定:“电子签字系指在数据电文中,以电子形式所含、所附或在逻辑上与数据电文有联系的数据,它可用于鉴别与数据电文相关的签字人和表明签字人认可数据电文所含信息。”

电子签字的概念意图指出,电子签名与手写签字具有相同用途,这些用途是为了鉴别个人以及将之与文件的内容联系起来。将电子签字界定为能够表明认可信息,这主要是为了确定一个技术先决条件,以便承认某项技术手段能够等同于手写签字。但是,对电子签名所运用的技术方式几乎没有规定,凡是具有一定鉴别作用的,满足技术先决条件的数据都可成为电子签名的方式。联合国贸易法委员会《电子签字示范法》中电子签名的概念是广义电子签名概念的典型代表。

法律要求在商务活动中符合“签名”要求,实际上是要求实现上述一种或几种功能。基于此,《电子签字示范法》的起草者沿用了《电子商务示范法》所采取的“功能等同法”这样一种新方法,这种方法立足于分析传统手写签字要求的功能和目的,以确定如何通过电子商务技术来达到这些目的或作用。所以,法律只需要根据所要求实现的一种或几种功能,制定与之相适应的要求。某种电子签名只要满足特定的技术和法律要求,就可以实现所要求的一种或几种功能,就可以被认为符合书面形式的要求。这种方法就是“功能等同法”。

(二) 狭义电子签名

狭义电子签名,是以一定的电子签名技术为特定手段的签名,通常指数字签名,它是以非对称加密方法产生的数字签名。

^① 曾更莹. 网际网络上运用电子签名所涉法律问题研究[J]. 万国法律.

^② The United Nations Commission on International Trade Law Model Law on Electronic Autograph,简称《电子签字示范法》。2001年12月12日年联合国贸易法律委员会通过的《电子签字示范法》,是国际上关于电子签字方面最重要的立法文件。

之所以排除其他形式的电子签名,而只承认数字签名在法律上的有效性,主要是出于对各种电子签名安全性和实用性差异的考虑。

狭义电子签名支持者在对现有生成电子签名的技术方法进行考察后认为,在现行的电子认证技术中,计算机口令容易被破获,其安全系数不足;对称密钥加密不适应开放型市场的需要;而笔迹、眼虹膜网等辨别技术应用成本过高,唯有非对称密钥加密(数字签名)方法,既安全可靠,又能适应开放型市场密钥分发的需要,而且成本也不太高,是较为理想的电子签名技术方案,因而应作为法定的电子签名技术予以确认。其他的电子签名技术的安全性,尚未被验证认可,或者不具有实用性,所以不应赋予法律效力。

通过立法明确肯定数字签名这一项技术的另一个理由是:泛泛地确认电子签名技术在满足一定的技术条件后具有法律效力,会使得广大消费者在判断某项电子签名技术是否达到法定条件时面临困惑,不利于电子商务被广泛推广。而只肯定数字签名这项成熟技术,可以帮助消费者建立信心,使其可以无保留地信赖数字签名,从而推动电子商务的大众化。美国犹他州以《数字签名法》确认数字签名为有效的电子签名形式,是狭义电子签名概念的典范。

(三) 强化电子签名

强化电子签名,有时又称安全电子签名。它是指经过一定的安全应用程序,能够达到传统签名的等价功能的电子签名方式。其具体形式是开放型的,任何能够达到同一效果的技术方式,都可囊括在内。与上述广义与狭义的电子签名概念相比较,该电子签名概念是一种折中式的概念。

联合国贸易法委员会《统一电子签名规则(草案)》在第一条中规定:“强化电子签名,是指可以通过应用安全程序,或各种安全程序的结合对其生成之时的状况进行验证的电子签名,以保证该电子签名:①对于签署者所使用的目的是独特的;②可以客观地证明数据电讯签署者的身份;③由签署者或以签署者独占控制的方式生成并附加于数据电讯;④是与数据电讯如此紧密联系的,即一旦数据电讯有任何变化,就会被反映出来。”但是,联合国贸易法委员会正式颁布的《电子签字示范法》第三条规定:“除第五条外,本法任何条款的适用概不排斥、限制或剥夺可生成满足第六条第一款凡法律规定要求有一人的签字时,如果根据各种情况,包括根据任何有关协议,使用电子签字既适合生成或传送数据电文所要达到的目的,而且也同样可靠,则对于该数据电文而言,即满足了该项签字要求。所述要求或符合适用法律要求的电子签字的任何方法的法律效力。”其根本原则是不歧视任何电子签字方法,即所有技术在是否满足特定的技术要求方面都被给予同样的机会。因此,如果符合法定要求,电子签字的电文与手写签字的书面文件之间,或各种电子签字的电文之间将同等对待。也就是说,联合国贸易法委员会放弃了强化电子签名的立场,而完全支持广义电子签名的概念。

(四) 我国法律上电子签名的含义

《中华人民共和国电子签名法》^①(以下简称《电子签名法》)第二条第一款规定:“电子

^① 《中华人民共和国电子签名法》由中华人民共和国第十届全国人民代表大会常务委员会第十一次会议于2004年8月28日通过,自2005年4月1日起施行。

签名,是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的信息。其中数据电文是指以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。”这表明,我国采用的是广义的电子签名概念,与联合国贸易法委员会《电子签字示范法》保持了一致。

在《电子签名法》出台前,《中华人民共和国合同法》(以下简称《合同法》)避开了电子签名问题,提出另一办法,即“签订确认书”。这实际是避开了必须有确定身份的“电子签名”的问题,这个方法属于“形式等同法”,而不是《电子商务示范法》采用的“功能等同法”。签订确认书并不能使电子合同完成签字人或依赖方认证的要求,电子合同也根本无法摆脱手书签名法律的束缚。^① 根据“后法优于前法”的规则,《电子签名法》中的规范将取代《合同法》的相关规范。

收到附有签字的数据电文的收件人,通常也认为是电子签名依赖方。《电子签名法》第三十四条第(二)项规定:“电子签名依赖方,是指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人。”

二、电子签名的分类



学前思考

电子签名为什么要有这样的分类呢?这样分类的作用又是什么呢?

目前,比较通用的电子签名机制是建立在公用钥匙基础结构问题和公用钥匙基础结构术语上的,这种签名被称为数字签名。当然,其他依靠非公用钥匙加密技术的电子签名的发展也是不容忽视的。

(一) 依靠非公用钥匙加密技术的电子签名

与使用公用钥匙加密的“数字签名”一起,还存在着各种其他装置,也包括在广义的“电子签名”机制概念中,这些装置可能现已投入使用,或考虑今后使用,以期履行上述手写签字的一种或数种功能。

1. 电子化签名

电子化签名技术将采用以手写签字为基础的生物统计学装置进行认证。在这种装置中,签字人将亲手签字,使用一支特殊的笔,书写在计算机屏幕上或数字输入板上,然后由计算机分析手写的签字并作为一组数值储存起来。这种签字可以附在数据电文之后,由收件人显示出来加以认证。这种认证体系将有一个先决条件,即手写签字的式样事先已由生物统计学装置做过分析并储存下来。现在已经有很多电脑公司推出电子签名使用的软硬件设施,美国也有许多百货商店开始使用这些设施来让消费者签署信用卡。

^① 李雅芳. 我国电子商务立法现状、问题及建议[J], http://www.china.com.cn/zhuanti2005/txt/2002-03/27/content_5123901.htm, 2013. 7. 3.

2. 生理特征签名

生理特征签名技术是基于用户的指纹、声波纹、视网膜结构等独一无二的生理特征的签名方法。这种签名方法要通过一定的设备识别上述生理特征,并运用一定的计算方法将生理特征转化为电子资料,并与预先建立的庞大数据库内的数据对照,以确认身份。但是,这种技术需要预先搜集大量生理特征数据,并且设备较为昂贵。目前仍在小范围内使用。

(二) 依靠公用钥匙加密的数字签名

依靠公用钥匙加密的数字签名,即数字签名。简单地说,发文者必须先制作一组“钥匙”,钥匙实际上是一长串像密码一样的数字,可以存储在硬盘、软盘或集成电路卡等介质中。这组钥匙,一个为私人钥匙,即产生数字签名的钥匙,此为发文者专有,另一个为公用钥匙,应由所有的收文者知悉,收文者凭此检测收文是否被篡改。做法是随着原始信息发送以私人钥匙加密的签名,以此向接收方保证,接收方收到的每一个字都与发送方所发的相同。数字签名与数据加密完全独立发送方计算出的签名和数据一起传送给接收方,签名值是关于发送方的私人钥匙和要发送的信息的一个数学函数的值。算法的构造保证如果不知道私人钥匙的话就不可能计算出这个签名值。接收方可以通过依赖发送方的公用钥匙、签名值和接收到的数据的另一个数学算法来验证接收到的信息就是发送方签名的信息。

三、数字签名



学前思考

张某是一名学习电子商务的大学新生,对于很多既陌生又新鲜的新词汇,他都不太理解。什么是数字签名?数字签名就是把自己的签名写在纸上然后上传到计算机里吗?数字签名要加密吗?签名能伪造吗?客户端不是有密码就行吗?怎么还有公钥和私钥?请你学习下面的知识帮助张某解决上面的这些问题。

(一) 相关概念和术语

1. 加密

数字签名采用加密方法创建和核查。加密是应用数学的一个分支。加密技术的应用比较广泛,比如IE浏览器就使用了128位的密钥。

在数字签名过程中,运用某种加密方法将电文转换为表面上不可懂的形态,收件人收到后再次利用加密方法将之还原为原有形态,这将保证传送中的信息即使被第三者拦截,第三者也是无法解读的。数字签名使用所谓的“公用钥匙加密法”,常常依靠算法函数产生两套不同但数学上相关的“钥匙”(即利用一系列数学公式产生的大数乘以素数)。其中一套钥匙(私人钥匙)用于产生数字签名或将数据转变为表面上不可懂的形态;另一套钥匙(公用钥匙)用来核查数字签名或将电文还原为原有形态。利用这两套钥匙的计算机设备和软件常常合起来称为“密码系统”。