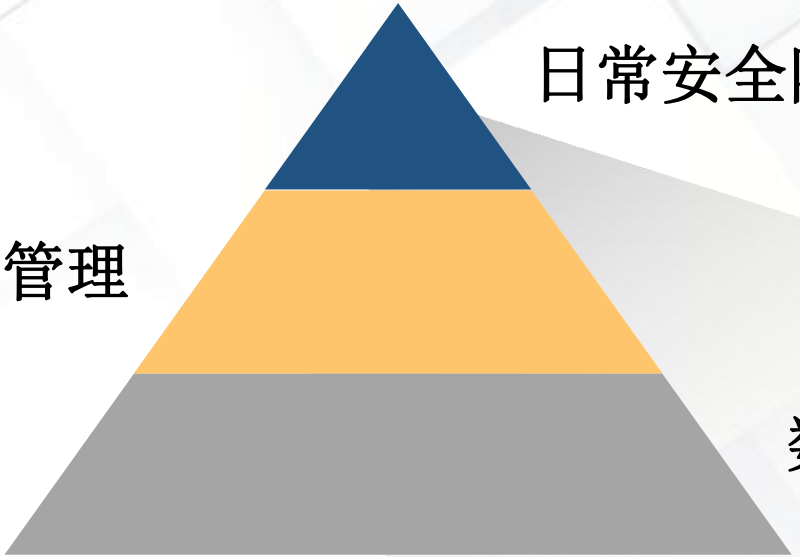
03 电子商务安全管理


日常安全防范
法律制度管理
数字证书认证中心

一、数字证书认证中心

实现网上安全支付是顺利开展电子商务的前提，建立安全的数字证书认证中心（Certificate Authority，CA）是电子商务的中心环节，其目的是加强数字证书和密钥的管理，增强网上交易各方的相互信任，提高网上交易的安全性，控制网上交易的风险，从而推动电子商务的发展。

（一）认证中心

在电子交易中，无论是数字时间戳服务还是数字证书的发放，都不是交易双方自己能完成的，而是需要具有权威性和公正性的第三方机构来完成。认证中心就是承担网上安全电子交易认证服务、签发数字证书并确认用户身份的服务机构。

国内的数字证书认证中心主要有行业、地方政府部门或企业等联手合作建立的数字证书认证中心，如中国金融认证中心（CFCA）、海关联盟认证中心（SCCA）、上海数字证书认证中心、广州市电子签名中心和山西数字证书认证中心等。

认证中心的主要功能如下：

- 证书的颁发
- 证书的更新
- 证书的查询
- 证书的作废
- 证书的归档

（二）数字证书

1．数字证书的定义

数字证书又称为数字凭证或数字标识，是由认证中心发行的、能提供在互联网上进行身份验证服务的电子文档。人们可以用它来表明自己在互联网中的身份或识别对方的身份。数字证书的格式遵循ITU的X.509国际标准，X.509标准数字证书包含以下内容。

（1）证书拥有者的姓名。

（2）证书的版本信息。

（3）证书的序列号，同一身份验证机构签发的证书序列号唯一。

（4）证书所使用的签名算法。

（5）证书发行机构的名称。

（6）证书的有效期限。

（7）证书所有人的公开密钥。

（8）证书发行者对证书的签名。

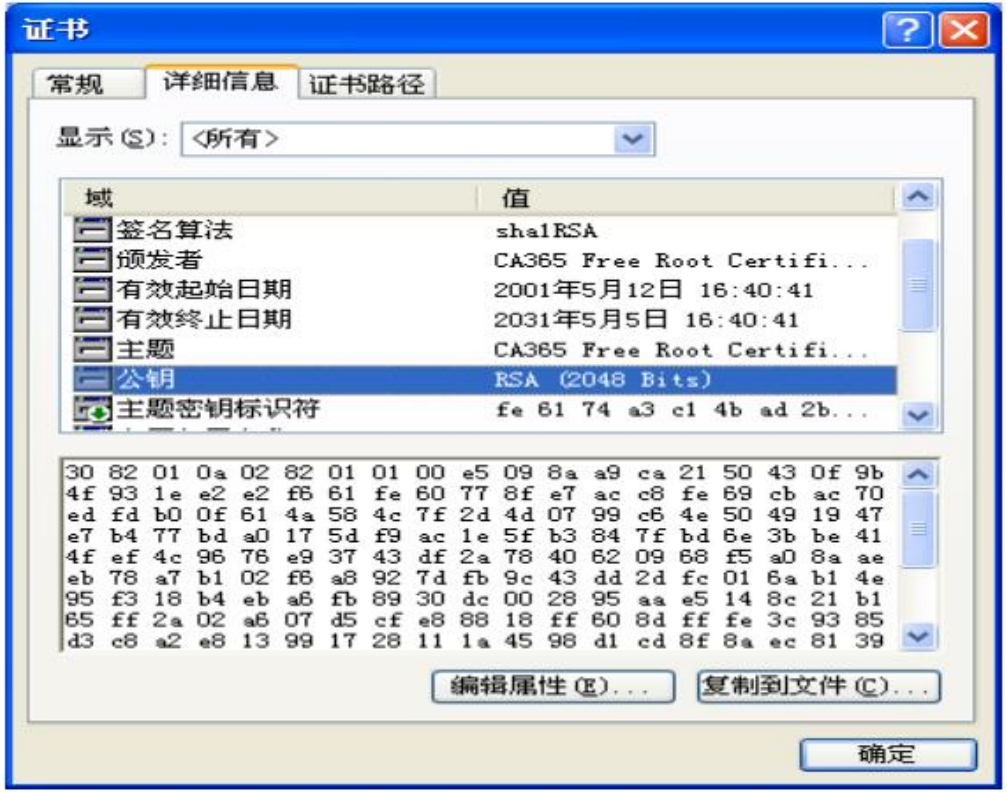
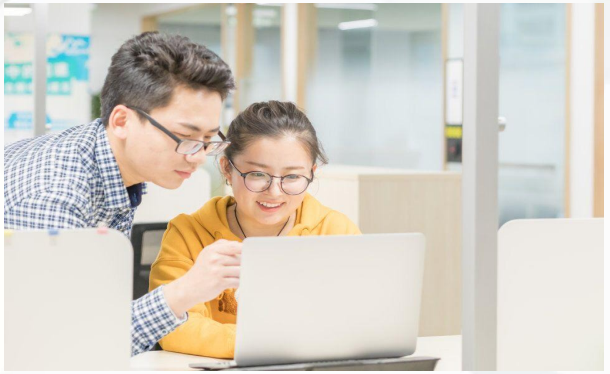


图8.5 数字证书示例

2．数字证书的分类

服务器证书

电子邮件证书



客户端证书

学而思，思而学

密信 MeSince 是沃通子公司2018年推出的加密电子邮件客户端软件，该软件支持Windows/安卓手机和苹果手机，全自动申请和配置电子邮件加密证书，全自动加密每封邮件，全自动为每封发出的邮件盖上时间戳。

3．数字证书的应用

- 用户在需要使用证书的网站上进行操作时，必须准备好装有证书的存储介质
- 如果用户是在自己的计算机上进行操作，则操作前必须先安装认证中心的根证书
- 操作时，系统会自动提示用户出示数字证书或者插入证书存储介质
- 使用完毕后，用户应记住取出拔除证书存储介质，并妥善保管

视野拓展

根证书

根证书是认证中心给自己颁发的证书，是信任链的起始点。根证书是一种特殊的证书，它的签发者是它本身，下载根证书就表明用户对该根证书以下所签发的证书都表示信任，在技术上则是建立起一个验证证书信息的链条，证书的验证追溯至根证书即结束。所以，用户在使用自己的数字证书之前必须先下载根证书。

视野拓展

支付宝数字证书

支付宝数字证书是使用支付宝账户资金时的身份凭证之一，可以加密用户的信息并确保账户和资金安全。用户申请后，在进行付款和确认收货等涉及资金的操作时，就会验证计算机上是否安装了数字证书。即使用户的账号被盗，对方没有相应的数字证书也动用不了账户中的资金。

视野拓展

微信支付数字证书

在微信内按“支付—钱包—安全保障—数字证书”顺序进入数字证书页面，根据提示进行设置即可启用微信支付数字证书。启用微信支付数字证书的作用是：提高支付安全性；提高每日零钱支付限额。数字证书就相当于一个认证的程序。它会使你的微信账户更安全。

二、法律制度管理

我国主要的保障电子商务安全的相关法律与制度：

（1）确立电子签名的法律效力。2004年8月28日，全国人民代表大会常务委员会第十一次会议通过了《中华人民共和国电子签名法》，2005年4月1日起施行。这是我国推进电子商务发展，扫除电子商务发展障碍的重要步骤。该法被认为是中国首部真正意义上有关电子商务的立法。

（2）规范电子认证服务行为。2005年1月28日，中华人民共和国信息产业部第十二次部务会议审议通过了《电子认证服务管理办法》，自2005年4月1日起施行。

（3）加强电子银行业务的风险管理。2005年11月10日，中国银行业监督管理委员会第四十次主席会议通过了《电子银行业务管理办法》，自2006年3月1日起施行。

点击视频：中国工商银行防诈骗宣传片

（4）规范网络商品交易及有关服务行为。2010年6月1日，中华人民共和国国家工商行政管理总局出台的《网络商品交易及有关服务行为管理暂行办法》中明确规定，通过网络开展商品交易及有关服务行为的自然人，应提交其姓名和地址等真实的信息。

（5）规范非金融机构支付服务行为，防范支付风险。2010年6月21日，中国人民银行出台了《非金融机构支付服务管理办法》，要求第三方支付公司必须在2011年9月1日前申请取得“支付业务许可证”，且全国性公司注册资本最低应为1亿元。该办法的出台意在规范当前发展迅猛的第三方支付行业。

（6）保障网络安全。2016年11月，第十二届全国人民代表大会常务委员会第二十四次会议通过了《中华人民共和国网络安全法》，自2017年6月1日起施行。电子商务安全相关法律与制度发展历程如图8.6所示。

（7）电子商务综合性法律。2018年8月31日，十三届全国人大常委会第五次会议表决通过《中华人民共和国电子商务法》，自2019年1月1日起施行。

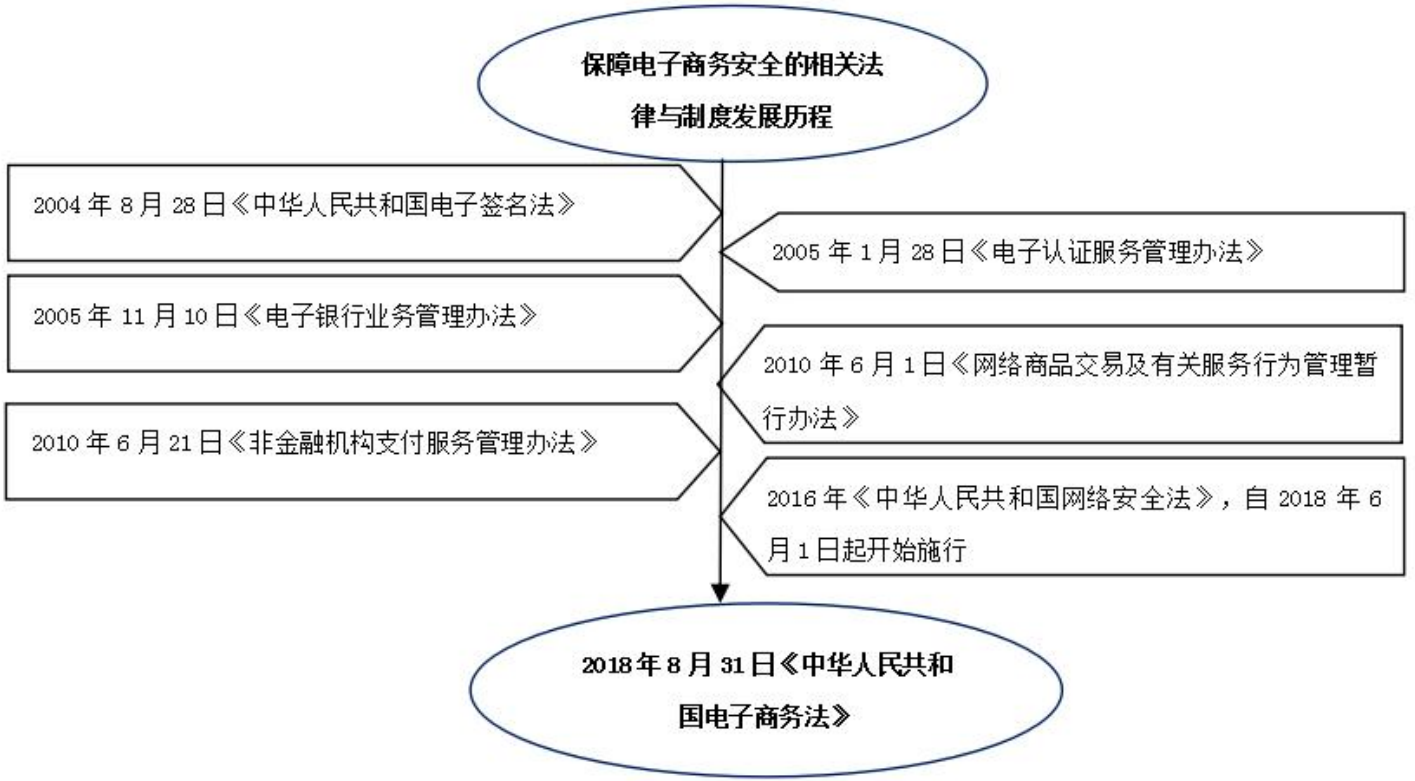


图8.6 保障电子商务安全的相关法律与制度发展历程

视野拓展

2019年1月2日，山西日报云媒体头条|《电子商务法来啦！10大亮点解读网络消费新变化》

三、日常安全防范

1. 计算机用户日常安全防范

2．移动端日常安全防范

- 谨慎下载安装手机软件和App程序
- 不要随便打开短信中的链接和扫描二维码
- 不要对手机刷机，以获取超级用户（Root）权限，或“越狱”
- 在公共场合，避免随意连接免费无密码Wi-Fi，否则可能会被黑客截取个人信息，甚至被植入木马病毒

视野拓展

Root和“越狱”

Root是安卓系统中唯一的超级用户，具有管理系统的所有权限。“越狱”其实等同于安卓平台上的Root，是指开放用户的操作权限，使得用户可以随意改写任何区域的运行状态，即利用“越狱”软件解除原有固件对手机系统的限制束缚，使用户可以自定义安装非官方或者来自第三方的应用程序。

实训案例

Office加密方式及文件保护

Word、Excel和PowerPoint是我们学习和工作中经常使用的三个Office软件。在使用它们提高工作效率的同时，也会让我们担心文档的安全性。因此，为了文档不被他人随意查看，可以利用加密技术为Office文档设置密码。下面以Word 2010为例进行介绍。

1．设置打开权限和修改权限密码

2．以只读方式打开文档

视野拓展

Office的密码保护

Office 2010的操作与其他版本的Office操作极为相似，为文档提供了四种级别的密码保护方式。

（1）第一级别是通过设置密码来决定用户是否有打开文档的权限。

（2）第二级别是通过设置密码来决定用户是否有编辑文档的权限。

（3）第三级别是通过对打开的Word文档启动强制保护，这样文档将以只读的方式打开。

Word、Excel 和 PowerPoint 都使用RC4的对称加密算法对受密码保护的文档进行加密。RC4是一种流密码算法，它对数据的每个字节进行操作，支持长度为40位、64位及128位的密钥，在为文档加密时我们可以指定密钥的位数。

归纳与提高

通过本章的学习，我们了解到在互联网上实现的电子商务交易必须具有保密性、完整性、不可否认性、真实性和可靠性等安全性要求。

一个完善的电子商务系统在保证其计算机网络硬件平台和软件平台安全的基础上，还应具备强大的加密和认证系统，以完成用户和信息的识别和鉴别，确保互联网交易和支付的可靠性、真实性、完整性，提供便捷的密钥管理，满足电子商务对计算机网络安全与商务安全的双重要求。

电子商务安全技术的提高、管理制度的完善、法律制度的健全需要政府和用户长期不懈的努力。个人用户和企业用户在互联网上开展商务活动时要注意进行网络防范。

谢谢观赏 第八章（完）