

# PDF与电子商务

主讲 田捷博士

(研究员, 博士生导师)

Email: [tian@dr.com](mailto:tian@dr.com)

<http://www.digiark.com/tian>

- 第一节 电子图书eBook的简介
- 第二节 两种主要的电子书格式
- 第三节 Adobe的epaper解决方案
- 第四节 PDA和手持eBook
- 第五节 PDF应用实例
- 第六节 电子商务和电子商务模式
- 第七节 在线支付手段
- 第八节 电子商务主要的安全要素

# 第一节

## 电子图书eBook的简介

eBook是electronic Book的缩写，它并没有严格的定义。不同的人给了它不同的定义，有些人把ebook定义为数字化的无纸的图书、文件、文档的内容；而有些人则把电子书定义为一种便携的、大容量的、容易使用的手持式电子设备。

我们倾向于后一种定义，从eBook的液晶显示屏上可以非常方便的实现阅读功能，也可以象传统书一样加注释、书签等，电子书可以很容易地实现从网上购买数字化的图书。出版商可以将图书加工成电子书放到网上供读者购买。电子书专用的服务器可以提供安全交易服务。读者除了可以用电子书设备读书，也可以用PC机上的阅读图书。





Franklin's new BookMan book readers

# 一、电子图书的几大优势：

## 1、直接：

随时拥有自己喜欢的书籍；直接按照需要下载图书，不需要花费时间去递送、打印、保存入库；

## 2、自由：

可以在任何地方任何设备上阅读；不需要担心书本的破损；轻松地同时携带多本书；

### 3、交互性强：

可以方便地添加注释、评论、书签等；

### 4、查询容易：

很容易就实现了传统图书无法解决的问题：查找功能；

## 二、电子书目前支持的文件格式

目前电子书支持的文件格式主要有OEB、PDF、TXT、HTML、LIT等几种。

### 1、OEB

OEB是Open eBook的缩写，不属于哪一家公司的产品，而是一种公开的基于XML标准；

## 2、PDF

PDF是Adobe公司提出的文件格式，Adobe公司提供了免费的浏览工具：Adobe Acrobat Reader；

## 3、LIT

LIT是微软提出的一种文件格式，微软提供Microsoft Reader浏览工具。我们主要介绍两种主要的文件格式PDF和LIT。

## 第二节

# 两种主要的电子书格式

目前电子书的格式主要有Adobe的PDF格式和微软公司的Microsoft Reader格式。两种格式各有千秋，下面逐一介绍。

一、 Adobe PDF格式：\*.pdf

二、 MS READER格式：\*.lit

# 一、Adobe PDF格式：\*.pdf

PDF格式是 Portable Document Format 的缩写，是Adobe公司推出的一种文件格式，自从1994年推出以来，已经成为一种被国际上大多数公司所接受的工业标准。PDF格式文件是目前互联网上使用最为广泛的文件格式之一。在电子文档领域，adobe公司一直以来都处于领先地位。

围绕着PDF格式，Adobe公司还提供多种转换工具以及Acrobat SDK，方便用户实现自己的PDF文件。Adobe还提供了免费的浏览工具Acrobat Reader。PDF是一种完美的电子文档发布格式，因为他克服了一般电子文件中经常遇到的各种问题：

## 通常电子文件中常见问题

## Adobe PDF 解决方案

收件人因为没有相应的创建文件时所用的应用程序而不能打开或阅读文件

任何人在任何地方都可以打开一个 PDF 文件，唯一需要的是免费的 Acrobat Reader 浏览器

由于平台、软件或版本的不同丢失了远文件中的字体、色彩或文件格式信息

通常 PDF 文文件中使用的字体是内置于 PDF 档案之中，PDF 总是以创建时的形式来显示，而不管字体、软件和操作系统是否与创建时一致

由于打印机或软件的限制导致文档不能打印

PDF 能够在任何打印设备上准确地打印出来

# 1、特点

总之，PDF具有以下几个特点：

- ◆ **CoolType显示技术**：明显地提高了水平方向的分辨率；
- ◆ **视觉保真性**：PDF中的电子页保留了印刷页的精确的内容：字体、图片元素、页面完整无缺。任何格式的书都可以以原有的面貌出现在PDF文件中；

- ◆ **视觉丰富**：文本和图像元素在文件中以最高分辨率形式出现。对视觉丰富的电子内容来讲，PDF是最为完美的，这种丰富性正好满足反映创作者意图和意愿的艺术、设计等领域。

- ◆ **跨平台、与操作系统无关**：这也正式PDF格式的“便携”性的表现。PDF文件的信息是“内含”的，甚至可以把字体、多媒体“嵌入”文件中，使PDF文件成为完全“自给自足”的电子文档。即无论在任何机器、任何操作系统下都能够以制作者所希望的形式显示和打印出来，表现出了跨平台的特性；

- ◆ 支持图书的页、目录、索引、标注等对象，基于PDF的eBook允许读者添加注释和各种标记，甚至可以添加声音注释；
- ◆ 支持文字编辑、图文混排及排版，支持PostScript格式；
- ◆ 结构开放，支持对象定义，可以添加视频、声音等多媒体对象，扩展了电子图书和电子文档的功能；

- ◆ 支持文档的发布管理、权限控制等，可通过相关的设置实现高效的文档管理；
- ◆ 客户端仅需要功能丰富的Acrobat Reader浏览器，支持各种阅读操作，包括：翻页、缩放、翻转、标注等等。
- ◆ 可以在任何地方发布：打印、添加到e\_mail中、粘贴在web站点上、或刻写在CD\_ROM；

- ◆ 采用几种压缩方式，使得文件结构紧凑，便于在互联网上的发布，同时支持在WEB上按页传输、浏览的功能，以降低用户浏览时的等待时间。
- ◆ 任何文件包括扫描的图像都可以用Adobe公司相应的工具转换为PDF文件，而不会丢失任何原有文件的信息。

## 2、PDF与HTML的区别：

正如前面提到的一样，PDF所包含的多媒体信息是内含的，就好象用WORD编写的DOC文件，图象、图表等等文件都保存在DOC里面，而HTML包含的多媒体信息则是外部的链接，不存放在文件的里面。

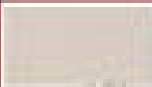


实际上，PDF与HTML最重要的不同，在于PDF文件可以实现“定稿后全封闭”。所谓“定稿后全封闭”，就是说在PDF编辑器中，我们可以将PDF文件设置为无法打印、无法选定、无法修改，这样就可以保证我们精心编辑制作的文本不会被任意篡改和复制，也就杜绝了转载成不同版本的可能性。

## 二、MS READER格式：\*.lit

MS Reader则是微软用于台式机和手持设备的eBook阅读软件。首次利用了ClearType™显示技术，ClearType™用于LCD显示器的低像素显示技术，低像素显示改变了红、蓝、绿三种基础色在LCD显示器上的像素值，比传统显示效果好。

ClearType是由MS Reader中的主要技术革新。microsoft reader也非常注重传统印刷的特点，例如：足够的空白边、适当间距、以及书签制作、高亮和注释等。其设计目标是尽可能地使屏幕阅读接近与传统书本阅读。MAREADER并不是要代替传统的书本，他只是让那些经常使用桌面PC机和膝上电脑以及更小的设备的人更加方便地来阅读书籍。MS READER界面如下：

# Library

		A Tale of Two Cities	Tuesday, October 02, 2001
Sort			
Search			
		Travels	Tuesday, October 02, 2001
		et Letter	Opened: Tuesday, October 02, 2001

- by Ititle
- by Author
- by Last Read
- by Book Size
- by Date Acquired

## 1、MS READER产品特征：

提供不可匹敌的阅读效果和阅读感受。

- ◆ ClearType™：ClearType™显示技术使得屏幕阅读更加舒适、清晰；



Annotations Index（注释索引）：  
Microsoft Reader跟踪你所做的所有的注释，包括书签、高亮显示、标记和划线。你可以从一个地方方便地看到你的所有的注释，同时还可以对注释进行编辑、删除、组织等工作；

- ◆ **Library**：所有的书和资料都保存在MicroSoftReader库中，你只要轻点标题就可以方便地浏览和阅读。同时在库中你还可以根据著作者、书的大小、最后一次阅读时间等项来对书进行整理和组织；
- ◆ **Bookmark**：Microsoft Reader可让你增加电子书签，并最高效地运用它，你可以直接从一页中删除书签，也可以改变它的颜色。所有的书签都在右边的空白处；

- ◆ **Easy Navigation** : Microsoft Reader 允许使用键盘或鼠标在一本书中自由地移动，你可以直接到指定的页中，也可以快速地前翻和后翻；
- ◆ **Search** : 电子图书一个最大的优势就是可以在一本书中方便地查找一个单词或一句话，在传统的书本中这是不可能实现的；

- ◆ **Highlighting** : 用鼠标高亮显示一个单词或一段话，并从几种颜色中选择一种来对高亮的内容进行编辑。可以在爷中直接删除高亮；
- ◆ **Dictionary** : 借助于Encarta Pocket Dictionary，你只需轻点就可以得到所需要的解释；

- ◆ **Notes**：你可以利用键盘轻松地对任何页添加评论；
- ◆ **FontSize**：Microsoft Reader允许你能即时地改变字体大小，创建所需要的大的打印版本；
- ◆ **Drawings**：可以对文本增加下划线、加圈以及任何类型的标记

## 2、系统要求：

### 操作系统：

- ◆ Microsoft Windows® 95,
- ◆ Microsoft Windows 98 Second Edition,
- ◆ Windows Millennium,
- ◆ Microsoft Windows NT ® 4.0,
- ◆ and Microsoft Windows 2000 Professional and
- ◆ Microsoft Windows 2000 Server operating systems.

## 其他系统要求：

- ◆ Pentium 75 或更高的微处理器；
- ◆ 16 MB 内存；
- ◆ 13 MB 可用的硬盘空间(Microsoft Reader占用6.75 MB 但安装时需要更多空间)；
- ◆ 装有 Microsoft Internet Explorer 4.01 with Service Pack 1 或更高版本；
- ◆ VGA or 更高分辨率显示器，
- ◆ 256或更多色彩支持的显示卡

### 3、MS READER与PDF比较：

	PDF 格式	MS READER 格式
操作系统	任何操作系统	微软的 windows 操作系统
动态阅读支持	不支持	支持
加注释功能	完备	完备
移动页的便捷性	方便	很方便
其它软件要求	无	要求有微软 IE4.0 以上版本
与第三方的兼容	很好	一般
多媒体信息加入的便捷性	方便	方便
阅读舒适性	一般	很好
符合传统习惯	一般	较好
显示技术	cool Type	clearType
查找功能	有	有
注释管理	无	有
原有面貌的保真性	精确	无

Microsoft Reader的LIT文件格式不同于PDF，虽然PDF是一种很好的文件格式，但它是静态的，不能很好地支持缩放功能；而Microsoft Reader采用动态阅读机制，即它能动态地缩放来适应你所使用的屏幕的尺寸，符合传统阅读习惯。目前，微软提供几种转换工具可以实现HTML格式和微软的Word格式到Microsoft Reader格式的转换，其他的转换工具也会在以后的日子里相继推出的。

。

最简单的制作Microsoft Reader格式的文件的方法是利用Microsoft Reader add-in for Microsoft Word中的Read功能，可以很方便地利用Word把文件保存为Microsoft Reader格式的文件。这个add-in可以从微软网站上下载。当前的Microsoft Reader版本支持文本、图像、声音等多媒体信息，将来的版本回支持视频流等其它多媒体信息。

总之，Microsoft Reader 的主要优势在于阅读的舒适性上，即阅读时没有滚动，翻页今需轻点按钮；页面形式与书本相同；ClearType显示技术使得屏幕阅读更加清晰和舒适。但它也有其不可克服的缺点，那就是仅仅能在微软的windows操作系统下运行，不具有平台的独立性，同时它还需要IE4.0以上版本的支持方可浏览。

# 第三节

## Adobe的epaper 解决方案

基于epaper解决方案，可以放心地通过web、intranet、email或CD-ROM来发布任何格式的文档，并可以在任何计算机上浏览和打印文档。不管你原来的文档是文本文件、纸文档甚至web站点，你都可以在PDF文件中保留原有的信息。

PDF文件格式是Adobe的epaper解决方案的核心，它的特点在前面已经介绍过了。

epaper的主要产品：

- 一、 Adobe Acrobat 4.0 主要特征
- 二、 Adobe<sup>®</sup> Acrobat<sup>®</sup> Reader<sup>®</sup>
- 三、 Adobe<sup>®</sup> Acrobat<sup>®</sup> Business Tools主要特征
- 四、 Adobe<sup>®</sup> Acrobat<sup>®</sup> Capture<sup>®</sup> 3.0
- 五、 Acrobat Web server 的主要特征
- 六、 Adobe<sup>®</sup> PDF Merchant<sup>®</sup>
- 七、 Adobe<sup>®</sup> Acrobat<sup>®</sup> Distiller<sup>®</sup> Server software特征
- 八、 Adobe<sup>®</sup> Acrobat<sup>®</sup> Messenger<sup>®</sup> Software特征
- 九、 Web Buy
- 十、 Create Adobe PDF Online

# 一、Adobe Acrobat 4.0 主要特征

- ◆ 把任何文档转换成Adobe PDF格式的文件
- ◆ 标记和注释PDF文档
- ◆ 提供安全选项和数字签名
- ◆ 创建PDF Web窗体

- ◆ 把PDF 文件整合到Web server或email中
- ◆ 在PDF文件中对后期的文本和图片进行编辑
- ◆ 从PDF文件中重用文本、图片、和表  
单数据
- ◆ 保留和打印PostScript® 图片

## 二、Adobe® Acrobat® Reader®

- ◆ 提供在所有平台上浏览和打印PDF文件，是一个免费的软件；

# 三、Adobe® Acrobat® Business Tools主要特征

- ◆ 创建Web页或站点的Adobe PDF "snapshots"
- ◆ 用电子markup工具对PDF文档注释；
- ◆ 数字签名和口令保护

- ◆ 用Acrobat Search在PDF文件的索引目录查找信息；
- ◆ 从PDF文档中拷贝或粘贴文本和表格到Word 或Excel中；
- ◆ 自动地把PDF文件附加到邮件中；

# 四、Adobe® Acrobat® Capture®

## 3.0

与扫描仪协同工作，把扫描文件转换成可以搜索的PDF格式，主要的特征有：

- ◆ 把扫描文件转换为可搜索的PDF格式；
- ◆ 创建可重用的的处理文档；

- ◆ 正确执行OCR、字体和页确认；
- ◆ 自动地创建内部文档连接；
- ◆ 用新的QuickFix工具高效校正OCR文本；
- ◆ 用新的Zone工具定义扫描页的图像区域、文本区域甚至关键字区域；
- ◆ 降低了处理的工作量，支持多处理器功能；

## 五、Acrobat Web server的主要特征

- ◆ 使得PDF内容能被第三方的搜索引擎更容易访问；
- ◆ 浏览PDF文件目录，浏览用户可选择  
的元数据；
- ◆ 转换PDF文件到HTML格式；
- ◆ 提供基于服务器的打印和传真PDF文件；

## 六、Adobe<sup>®</sup> PDF Merchant<sup>®</sup>

- ◆ 基于服务器的软件，是发布商、代理商和零售商更容易对PDF文档进行加密处理并在Web上销售；

# 七、 Adobe® Acrobat® Distiller® Server software特征

- ◆ 简化PostScript-to-PDF文件转换，通过Distiller 的job设置的集中控制来保证一致处理；
- ◆ 通过把PDF处理任务移动到网络服务器上节省创建时间；
- ◆ 在UNIX机器上创建PDF文件；

# 八、Adobe® Acrobat®

## Messenger® Software特征

- ◆ 仅通过轻轻一点来创建可搜索的文档；
- ◆ 以Internet的速度来发布文件；
- ◆ 把文件以邮件的附件形式发送；
- ◆ 把文件传输到任何标准传真机上；

## 九、Web Buy

- ◆ 从web上下载加密的文件；
- ◆ 可以浏览和购买卖家用Adobe PDF Merchant创建的数字内容；

# 十、Create Adobe PDF Online

- ◆ 把各种格式的文件转换为Adobe PDF文件；

# 第四节

## PDA和手持eBook



- 一、PDA简介
- 二、PDA的分类
- 三、PDA的发展趋势
- 四、手持eBook
- 五、E-BOOK的发展历史



# 一、PDA简介



从广义上讲，PDA是Personal Digital Assistant的缩写，字面意思是“**个人数字助理**”。这种手持设备集中了计算，电话，传真，和网络等多种功能。它不仅可用来管理个人信息（如通讯录，计划等），更重要的是可以上网浏览，收发Email，可以发传真，甚至还可以当作手机来用。

尤为重要的是，这些功能都可以通过无线方式实现。当然，并不是任何PDA都具备以上所有功能；即使具备，也可能由于缺乏相应的服务而不能实现。但可以预见，PDA发展的趋势和潮流就是计算、通信、网络、存储、娱乐、电子商务等多功能的融合。



PDA一般都不配备键盘，而用手写输入或语音输入。PDA所使用操作系统主要有 Palm OS，Windows CE和EPOC。PDA的发端可以追溯到Apple公司于1993年推出的Newton Message Pad。之后不久，就有产商推出类似产品。目前，PDA的价格还偏高，但专家们相信，它将最终走进“寻常百姓家”，成为真正的“个人数字助理”。

从狭义上讲，PDA是指可以称作电子记事本，其功能较为单一，主要是管理个人信息，如通讯录、记事和备忘、日程安排、便笺、计算器、录音和辞典等功能。而且这些功能都是固化的，不能根据用户的要求增加新的功能。



广义的PDA主要指掌上电脑，当然也包括其他具有类似功能的小型数字化设备。掌上电脑一词也有不同解释。狭义的掌上电脑不带键盘，采用手写输入、语音输入或软键盘输入。而广义的掌上电脑则既包括无键盘的，也包括有键盘的。不过，在中国市场，几乎所有的掌上电脑都不带键盘。在这里，我们从广义上来理解PDA。

## 二、PDA的分类



个人信息管理(PIM)类掌上电脑、  
功能型掌上电脑、无线通讯类掌上电脑。

**PIM类掌上电脑**主要包含记事簿、  
电话本和词典等功能，目前在国内市场  
上居主导地位。随着降价战的升级，  
PIM类掌上电脑将走向普及，市场份额  
将集中在少数品牌手中。

**功能型掌上电脑**主要是指具有强大的电子图书、多媒体、数据库、网络通讯等部分或全部功能，一般具有软件升级或硬件扩展能力的掌上电脑。基于WindowsCE、PALM、HOPEN、CELLVIC、PENBEX等操作系统的绝大多数掌上电脑可以归在这一类。电子图书型和面向行业应用型掌上电脑都在此列。

由于电子图书型掌上电脑的巨大市场前景，未来它将独立为掌上电脑的一类。这类掌上电脑市场能够容纳数量众多的品牌。国内功能型掌上电脑市场过去两年一直不如人意，2001年会随掌上电脑总体市场的迅速增长势头获得大幅度增长。

**无线通讯类掌上电脑**是指直接通过无线通讯网络提供内容和服务的掌上电脑，除了具有一般掌上电脑的功能外，还具有寻呼机或手机的功能。其中已经成熟的是寻呼PDA，国内已出现了8款寻呼PDA。明年的寻呼PDA市场将迅猛增长，市场容量由今年的20万台扩展到100万台左右。

### 三、PDA的发展趋势



- ◆ 与互联网和无线通讯的结合趋势；
- ◆ 个性化和本地化趋势；
- ◆ PIM类掌上电脑在降价战中走向普及；
- ◆ 无线通讯类掌上电脑市场迅猛增长；
- ◆ 无线通讯类掌上电脑市场迅猛增长；

- ◆ 功能型掌上电脑走出市场低谷，PALM和POCKET PC角逐高端；
- ◆ 电子图书型掌上电脑在摸索中前进；
- ◆ 越来越多的通讯和家电厂商推出掌上电脑产品；
- ◆ 新品牌层出不穷，LINUX异军突起；
- ◆ 嵌入式软件开发欣欣向荣。

## 四、手持eBook

这里所说的eBook是指一种便携的、大容量的、容易使用的手持式电子设备，从液晶显示屏上可以非常方便的实现阅读功能，也可以象传统书一样加注释、书签等，电子书可以很容易的实现从网上购买数字化的图书。

出版商可以将图书加工成电子书放到网上供读者购买。电子书专用的服务器可以提供安全交易服务。读者除了可以用电子书设备读书，也可以用PC机上的阅读软件图书。

我相信很多人都有阅读电子书的经验，这大概是PC和Internet普及带来的结果。网络给我们带来了大量的阅读材料，从小说到新闻，当你有了PC，你就可以打开一篇文档或网页，然后你可以慢慢地阅读下去。

但这样的阅读非常乏味，因为我们用的显示器，有个最大的问题——太闪烁，而解决办法就是买一台高档的显示器，调高刷新频率，这样你的眼睛基本可以长时间观看。一套好的读书工具也很重要，你需要更换底色、设置书签、自动滚屏等，好在PC上有那么多的软件开发者，读书的工具软件比比皆是。

那么用PC来看电子书真的很完美了吗？不！实际上，这种方式有个无法克服的缺点，如果你想躺在床上看书，或者走在路上边走边看，你能抱着十几公斤重的PC完成这一切吗？即使是笔记本电脑，恐怕也没有人这样做，太不方便了！我们需要更方便而专业的阅读工具。所以我们说EBook的标准：容易携带、容量大、阅读方便、交互性强。满足我们无论是坐者、躺者、还是站者都能够自由自在的阅读。

## 五、E-BOOK的发展历史

较早出现的专业电子书工具是SoftBook，尺寸大致与杂志类似，支持灰度显示，只要插上电话线就可以从SoftBook的服务网站上下载到电子书；

而NuvoMedia公司的Rocket eBook，它的尺寸更小类似于一本平装书，但仅仅能显示黑白两色，不支持灰度级。Rocket eBook没有内置Modem，它需要和PC的连接，通过PC上网下载电子书在传送到Rocket eBook上。此外，Rocket eBook还提供软件可以将PC上的文档转换后传送到eBook阅读。

最近美国纽约的PC Expo大展上，Franklin电子出版公司发布的eBookMan的大小就如同你的手掌，该有的PDA功能全都有，例如手写识别，语音记录，排定日程，与Outlook同步，它带一个单色的液晶显示屏，屏幕分辨率200 x 240 像素，带一个多媒体扩展槽，除了能读书以外还可以听MP3音乐，再加上与微软的合作，采用微软的clearType 显示技术，相信会更具有吸引力的。

在Pocket PC之前的传统Windows CE机型都需要一些第三方读书软件如MobiBook的支持，而有了Reader则使人们完全可以扔掉原来的电子书软件。Pocket PC主要由Casio、Compaq、HP三家大厂商开发及生产，包括彩色液晶显示器和立体声等先进功能，但价格很高，高达500到600美圆。

再来看另一个掌上电脑的大阵营 Palm，虽然Palm的屏幕显示技术不如 Pocket PC，但 Palm的机型普遍更加小巧、更加省电，液晶屏幕有16阶灰度级，长时间阅读也不觉得吃力。特别是Palm有庞大数量的软件支持。

总之，目前影响E-BOOK发展的几个因素是内容、阅读习惯、阅读舒适性、版权保护、价格(下载网费、PDA硬件)、用户群等。

# 第五节

## PDF应用实例

- 一、网络经营者的个人化策略
- 二、金融机构运用PDF办公
- 三、文件编制部门使用PDF节省  
巨大
- 四、新兴的一对一的出版方式

# 一、网络经营者的个人化策略

无数以服务消费者为主旨的网站都在残酷的竞争中努力求得生存，它们的实践证明了一对一向顾客提供服务的重要性。与顾客保持一对一服务的良好关系是任何一个商家业务取得长远成功的关键，不论在互联网上还是网下。

一些诸如 Lands' End 的网站在顾客下订单的过程中，客户服务代表与顾客会直接进行交流。这些网站庞大的在线数据库存有大量信息，可以回答困惑的消费者提出的几乎所有问题。

在顾客打来咨询电话时，客户服务代表会用 PDF 文档 e-mail 给顾客，这个 PDF 文档包括电话中涉及的一切内容，为顾客提供视觉印象，从而保证双方处于“同一界面上”。

不过，有效的客户服务不仅仅是在网上购物时能拉住顾客。注重个人服务的网站还应提供“一对一营销”服务，这才是最根本的。这些网站运用个人化工具，将顾客和客户服务代表置于同一界面，而且 Web e-tailers 传递的品牌信息明显的与众不同。

以前，客户服务管理部门(CRM)把传统的电话服务与互联网结合起来，现在，Adobe 公司的产品使商家与顾客的交流更丰富多彩，更注重个人服务，进行网上经营的众多公司正运用多种技术，力求将顾客放在第一位。

就建立最佳客户关系来说，公司仅仅设立 e-mail 客户服务系统或一个“常见问答”网页是不够的。立足互联网发展的公司还需要针对每个顾客的具体情况提供服务，包括有的顾客喜欢打电话直接与客户服务代表联系。

有一些公司，像 Quintus 和 Apac Customer Services(Apac 客户服务公司)，它们的客户服务管理部门(CRM)能够帮助商家把多种工具结合起来，更好的为顾客服务，同时也降低成本。据 Forrester Research 资料，运用 CRM 系统可使公司在客户服务方面削减高达 43% 的成本。

## 二、金融机构运用PDF办公

注重高质量的客户服务并推出不同的服务系列,使得 Pacific Life 已成为美国最大、最著名的金融服务机构之一。为加强这一优势,公司已意识到必须控制其纸张为基础的申请程序,转而提供一种方便快捷、成本低廉的途径将申请表发放到全国的金融专业人员手中。

解决方案：VALET ( Variable Annuity and Life Electronic Transaction ) ——一个创新的系统, 利用 Adobe Acrobat 软件和 Adobe 便携文件格式 ( PDF ) 将 CD-ROM 上的申请表单传递给金融专业人员, 或是通过安全的 extranet 进行传递. 完成的申请表单只需打印、签名, 就可返还给 Pacific Life, 然后再进行即时扫描, 纳入公司的客户档案。

## 1、自动选择表单

在具有严格规定的金融服务行业中，必须几百种表单以适应美国各个州不同金融服务的需要。对于单项服务来说，选择和提交正确的表单就有 17 种之多，这是件非常令人头痛的事。如果申请中有一份表单丢失，那么客户就不能完成此项服务的文书工作。

Pacific Life 的 VALET 服务加快了申请工作的完成，同时提高了服务的便捷性。运用 Adobe Illustrator Adobe Premiere 和 Adobe Photoshop 设计的友好、动态界面，会提示金融专业人员回答 8 个简短的问题，这些问题都是关于客户信息、所在地及其他相关资料。面对客户的反应，VALET 采用了 Adobe PDF 格式的表单，并将其整理合并成单个 Adobe PDF 文件。

如果客户是一名金融专业人员的固定客户的话，VALET 还会提供含有客户地址、社会保险及电话号码等等的 Adobe PDF 表单，这些内容都是从代理处的数据库中获取的。

VALET 的申请同样也利用了 Acrobat 中的 JavaScript 性能来核实表单字段中的数据。当表单完成时，代理处可点击按钮将资料储存在本地数据库中——在那里可快速、轻松地参考资料——然后将 Adobe PDF 表格打印下来，客户签名，再邮寄到 Pacific Life 处理。

## 2、事务部门无纸化办公

自动捕捉资料性能的运用对于工作流程的简化是非常重要的。在收到申请后。Pacific Life 运用 KODAK 扫描仪进行扫描。字符识别技术在每个字段中抓取资料，并自动将资料输入申请处理数据库中。同时将扫描的表格转换成 Adobe PDF 格式以便归档。

金融专业人员发送印刷整洁的 Adobe PDF 表单减少了以往字符识别所引起的问题。“由于表单在收到后 24 小时内就进行扫描,电话中心的工作人员可为客户提供最新、准确的帐户信息。”VALET 的项目经理 David Conway 说,“运用 VALET 加速了工作进程,如今我们接收的文书工作已无任何差错。行业中,从送支票到签发养老金的平均时间大约需要 5 天。而在我们的事务部门只需 24 小时或是更少的时间。这是一种竞争优势,我们的客户可获得即时服务,经纪人也能快速得到佣金。”

### 3、完美无缺的表格

Adobe Acrobat 和 Adobe PDF 为 VALET 提供了若干好处。而且这些好处都是不能从其他技术获得的。最重要的一点是 Adobe PDF 文件与原始纸张表单完全一致。全部的 Pacific Life 表单，都含有一个条形码——这是扫描软件用来识别表单类型的。

同时，Adobe PDF 文件的高保真性能为公司节省了重新编码原始光符识别这类例行公事的费用，而且重新编码的原始光符识别只能适用于表单特定的字段，如客户的姓名和电话号码等等。

## 4、比纸张文件更节省成本

VALET 系统提高了金融专业人员对 Pacific Life 养老金业务的兴趣，同时也减少了运作费用。同样，系统也消除了作废表单的费用。除了运作费用减少之外，在线表单的预计收入也是令人印象深刻的。“自从有了 VALET 和 Adobe Acrobat 后，纸张文件成本不断下降，我们也能更快地满足客户的要求，我们期望客户的满意程度有所提高。”

### 三、文件编制部门使用PDF节省巨大

今天愈来愈快速的产品推出的幕后英雄很可能是属于文件编制部门。归根结底，他们的职责是要去处理更多及更频密的产品推出文件编制工作往往在没有更多资源下去进行。所以很多文件编制部门好像 Texas Instruments (TI) 的 application-specific integrated circuit (ASIC)产品组以先进的文件创制及输送工具来面对挑战。

ASIC 产品资讯经理 Kathlyn Auten 说，有了 Adobe Acrobat, Adobe Portable Document Format (PDF), 及 FrameMaker, 我们已简化了我们的文件签署及查核程序，由印刷本转为网上为主的文件传送，而以同一数目的员工生产出四倍的文件输出。

TI 是全球半导体公司与及世界首屈一指的数码讯号处理及模拟科技的设计者及供应商。在 ASIC 部门，在德州的十名作者及印度的四名作者合成一组，创制高度技术化的数据书本、用户说明书及产品单张，以便消费者、电子厂商及电讯公司用作将 ASICS 融合在他们的系统内。

在 Adobe 的签署、查核及出版工具协助之下，这小组可以每两个月生产超过 15,000 页的文件。他们在去年九月生产了超过 34,000 页文件作输出。

Kathlyn Auten（左）及 Ann Balaban（右）使用 Acrobat、PDF 及 FrameMaker 来将 TI 产品文件在网上传送。这样做，他们能够生产及分发多四倍的文件与及节省大量金钱和时间。

《节省一百万美元》（Adobe FrameMaker），Acrobat 及 PDF 已戏剧化地减低了制作 TI 的数据书本的时间及开支。这些书本是介绍技术性资料例如运作情况及电力特徵等。TI 在过往使用一个程式去从其设计数据中抽出数据，然后将数据变成书本格式，以作出版及印刷。这程式开始后需时超过三个月才可完成书本，其中一个月是印刷，另外三个月是将档案转为 HTML 格式以便在网上出版。

计划经理 Ann Balaban 说，当我们从印刷厂收到这些材料时，它们已经过期了。纸张印刷的文件不但需要更多时间制作，而且对用户构成不方便。他们对于找寻某一问题的书本有困难，更不要说要解答这条问题了。

用纸张印刷的数据书本现时对于 TI 的 ASIC 文件处理组已是陈旧落伍了。该组现时已在公司的 intranet, extranet 出版其数据书本，亦在顾客的网址以 PDF 及 HTML 出版。

## 四、新兴的一对一的出版方式

AudienceOne 是新兴'一对一'出版市场的领先产品。通过以 Adobe(r) Acrobat(r) 方式储存的 PDF 文件中的资料,运用Adobe的软件和服务的公司可以制作出目的性更明确,更为个人化的印刷品或进行在线传输,增进与客户的关系。

Adobe与 Advanstar Communications 公司合作开发 PointeOne--一个基于互联网的信息站，参加贸易展览的参展商和杂志读者都可以在此编写他们感兴趣的内容。AudienceOne 软件会运用这些信息为每个人建立不同的公司和产品资料登记册。

Adobe在1999年5月举行的“印刷与出版技术博览会”上首次推出这项服务。在博览会上，有436个参展商制作了916本电子书籍，这些书籍都是由Agfa数字式印刷系统印刷、装订出来，并分发到各个楼层。超过50家参展商提供了PDF内容的方案，相应的，他们也节约了大量的成本，并且快速地抓住了关键的发展机会。

"一对一"印刷是一种满足个人用户需求  
的杰出方式，极大的削减了不必要的  
市场推广资料的浪费。PDF 是一种理  
想的格式，因为它使得在线校样，高质  
量的，可靠的数字式印刷都能够在一个  
工作流程中完成。除此之外，我们不可  
能通过任何其它方式做到以上几点。

# 第六节

## 电子商务和 电子商务模式

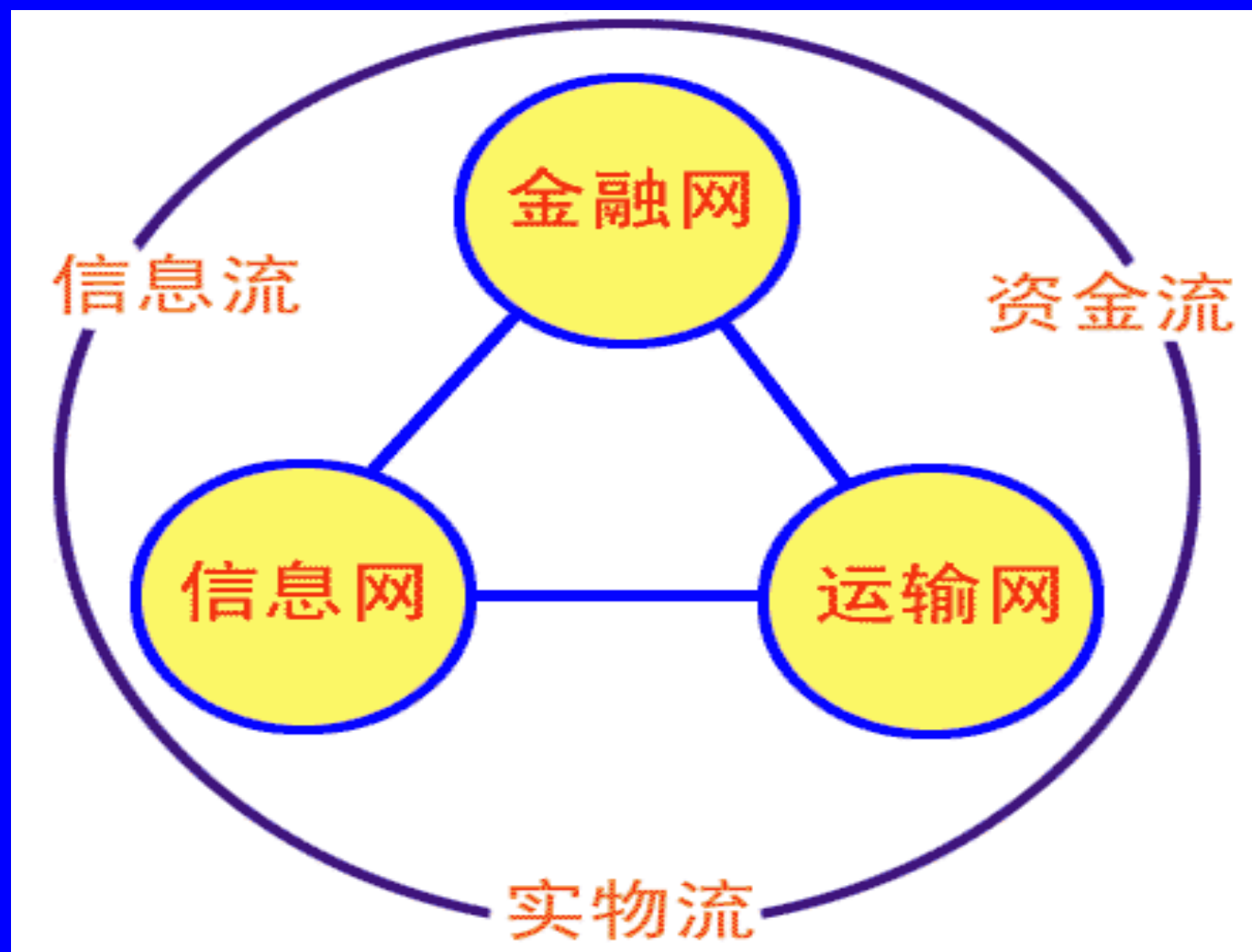
一、电子商务

二、电子商务模式

# 一、电子商务

## 1、电子商务的组成要素

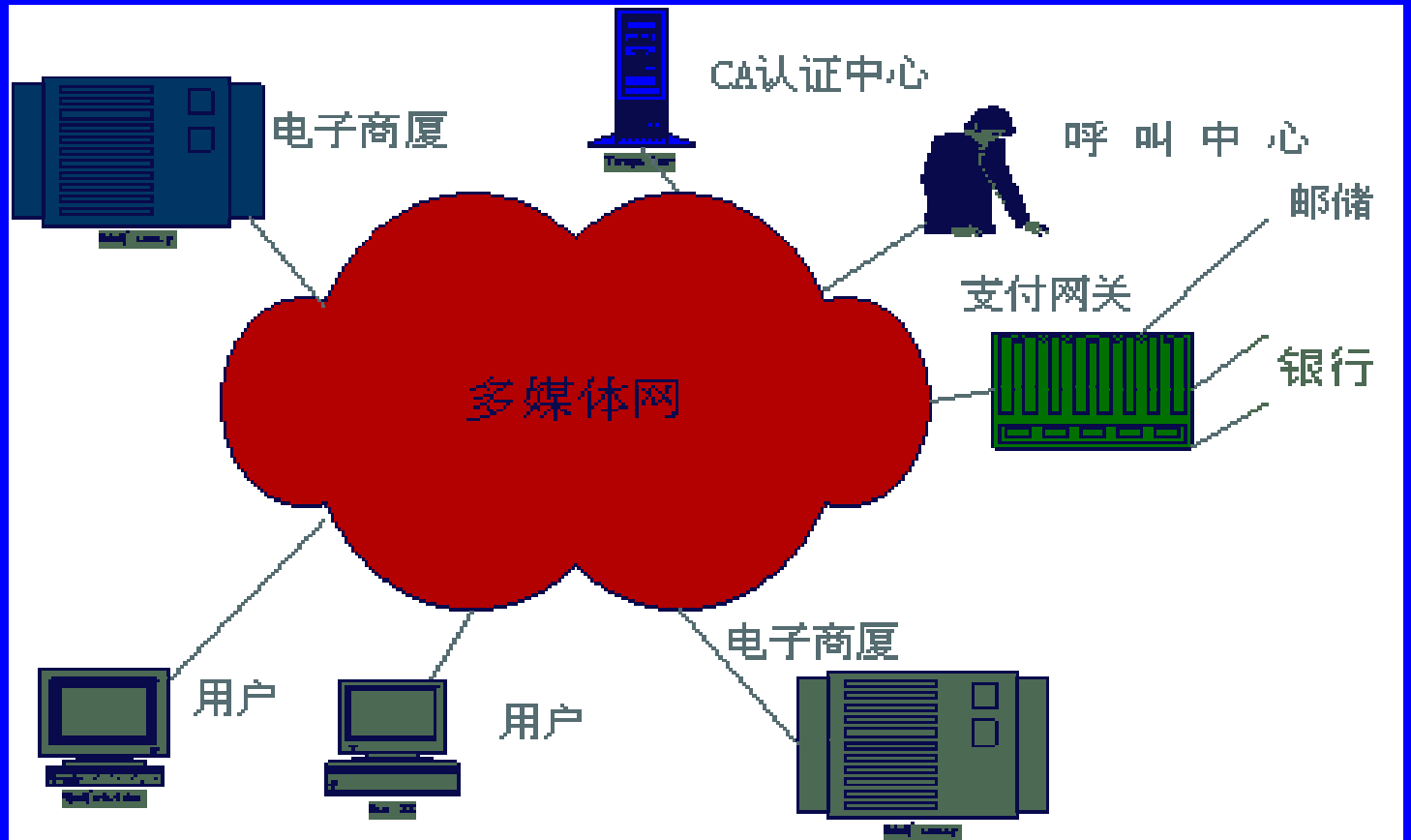
电子商务大系统包含三个关键组成要素



- ◆ 信息网：提供电子商务参与各方之间的信息传送与处理功能；
- ◆ 金融网：提供交易各方的在线或离线的支付功能；
- ◆ 运输网：当商品是实体时，如何从一方传递到另一方；

因此，很明显，在电子商务的系统中，有三种不同的“流”，也就是以信息网为载体的信息流，以金融网为载体的资金流和以运输网为载体的实物流。生流不息，商机不已。

## 2、 电子商务的系统结构



- ◆ 用户通过计算机或其他类型的终端如机顶盒等接入多媒体网
- ◆ 企业或政府通过电子商城发布信息
- ◆ 银行通过安全的支付网关提供在线的支付

这些用户、企业、银行等都是从安全电子认证中心获得数字证书，所有需要人工辅助的业务都由客户服务中心统一受理。同时，还需要组织一个完善高效的物流网络来进行商品的配送。

### 3、电子商务的分类

按是否发生支付：

#### I. 支付型电子商务。

所谓支付型电子商务，指的是有关银行参与商务活动的全过程并实时地进行支付转帐的电子商务。由Visa、MasterCard等公司建立的SET协议是目前最完整的网上交易和网上支付协议。

## III. 非支付型电子商务。

非支付型电子商务一般指非实时支付的电子商务。目前，大部分应用属于这一类，多数借助于SSL协议实现。

# 从参与对象上：

## I. 个人 - 企业：

网上购物(实物，信息，服务) 网上  
交费（电信、水电、煤气等）

## II. 企业 - 企业：

EDI、EOS、EFT、网上企业采购

### III. 个人 - 政府：

个人报税、资料处理

### IV. 企业 - 政府：

网上报关

## 电子商务给企业带来的优势：

- ✓ 降低交易成本
- ✓ 减少库存成本
- ✓ 缩短生产周期
- ✓ 增加商业机会。

## 二、电子商务模式

电子商务模式（Business Model）主要是指电子商务的不同类型，比如不同的交易对象、交易范围、解决方案、服务方式等。

- ◆ 按交易对象划分，可以分为B2B（企业对企业），B2C（企业对消费者），C2B（消费者对企业），C2C（消费者对消费者）B2C2C、B2C2B、C2C、B2A（Business-to-administrstions）等等；
- ◆ 按交易方式可以划分为定价模式、竞价模式、议价模式等，有人将竞价模式划分为拍卖和集体竞价模式。
- ◆ 按交易内容还可分为专卖店、商城/商厦/超市、交易市场/交易中心、行业/纵向市场、综合/横向市场、专业网站等等。
- ◆ 服务模式包括会员制和网上社区等。

# 1、B2B企业级电子商务

企业级（Business to Business）电子商务一般被简称为B2B的电子商务过程，它是一个将买方、卖方以及服务于他们的中间商（如金融机构）之间的信息交换和交易行为集成到一起的电子运作方式。B2B电子商务主要是进行企业间的产品批发业务，因此也称为批发电子商务。

传统上，基于EDI技术的B2B电子商务由于其巨额的开销，成为大的企业、大的银行以及大的合作伙伴之间的专利。但目前基于INTERNET的EDI技术的出现和各种网络支付手段的建立和完善使得中小型企业进入这一领域成为现实。简单的说，B2B企业级电子商务网站是批发业务，面对的是特定的公司，主要是产品的批发业务。主要目标是维持固定的客户。

另外，在INTERNET上实现B2B电子商务必须具备一定的基础，其主要表现在：

- I. 信息的标准化；
- II. 用户身份验证；
- III. 网络交易集成技术。

## 2、B2C企业对消费者电子商务

商业机构对消费者（Business-to-consumer）的电子商务，指的是企业与消费者之间进行的电子商务活动。这类电子商务主要是借助于国际互联网所开展的在线式销售活动。最近几年随着国际互联网络的发展，这类电子商务的发展异军突起。商业机构对消费者电子商务是近年来各类电子商务中发展较快的。其主要原因是国际互联网的发展为企业和消费者之间开辟了新的交易平台。

随着全球上网人数的不断增多，国际互联网的使用者已经成为企业进行电子商务的主要对象。从技术角度看，企业上网面对广大的消费者，并不要求双方使用统一标准的单据传输。在线零售和支付行为通常只涉及到信用卡、电子货币或电子钱包。

另外，国际互联网所提供的搜索浏览功能和多媒体界面，使消费者更容易查找适合自己需要的产品，并能够对产品有更深入的了解。因此，开展商业机构对消费者的电子商务，障碍最少，应用潜力巨大。就目前发展看，这类电子商务仍将持续发展，是推动其他类型电子商务活动的主要动力之一。

总之，B2C是企业通过网络，提供可客户各种交易和服务。客户利用PC机或其他上网工具连接到网络上后可以取得各式各样的在线即时服务，包括商品的查询、产品支持、在线订货等等。目前最常见的B2C模式就是网络商店，网络商店最大的好处就是全年无休的，但却省下了店面成本、水电开销，雇员开支、囤积货品的成本，而且网络商店的服务范围是全世界，加上上网人数的增加。

产品的竞争力是无法估量的，最重要的是不管企业规模的大小，都可以直接与客户接触！B2C电子商务网站是零售业务，它的客户是全社会的消费者的。其主要的目标是吸引消费者。

目前，一些国家已经制定了B2C电子商务的相关标准，制定这些标准的目的有五个：

- I. 增加消费者在INTERNET上进行交易的信心和满意程度；
- II. 建立消费者和销售商之间的信赖关系；
- III. 帮助销售商获得世界级的客户服务经验，加快发展步伐并降低成本；
- IV. 支持和增强INTERNET商务的自我调节能力；

V. 帮助销售商和消费者理解并处理迅猛增长的各种准则和符号。显然，这一标准既可以被销售商用于其INTERNET商务，并且向所有消费者和合作伙伴宣称自己符合这一标准；也可以被消费者用来检验销售商是否可以提供高质量的服务。同时，也可以指导如IT供应商、网站开发商、系统集成商等从事相关的业务。

例如，1999年12月14日世界上第一个INTERNET商务标准这些标准在信息中心、公布的内容、产品/服务、保密和安全、确认和通知、帮助和客户服务、其他共七个方面对B2C电子商务提出了最低的要求。

### 3、C2B消费者对企业（Consumer to Business）的电子商务

消费者对企业的电子商务是B2C的一种延伸。消费者通过团体购买的方式来买到价格相对较低的商品。

# 第七节

## 在线支付手段

在线支付手段的实用是普及电子商务实践的一个重要保证。在线支付需要主流金融机构全方位的支持方可附注于实际中去。

在因特网上做电子商务，支付方式可以是在线的电子支付（“一网通”等）；也可以采用离线的传统支付方式“网上贸易，网下结算”，如邮政、电传来用的方式。传统支付方式的优点是人们比较熟悉，感觉安全；缺点是效率低下，使电子商务失去了快捷的特点。因此，使用电子支付是电子商务走向成功的关键因素。

一、电子支付的特征

二、电子支付特点

三、电子支付模式

四、电子支付协议分类

# 一、电子支付的特征

- ◆ 电子支付是采用先进的技术通过数字流转来完成信息传输的，其各种支付方式都是采用数字化的方式进行款项支付的；电子支付的工作环境是基于一个开放的系统平台（即因特网）之中；
- ◆ 电子支付使用的是最先进的通信手段；
- ◆ 电子支付具有方便、快捷、高效、经济的优势。

## 二、电子支付特点

- ◆ 以计算机技术为支撑，进行储存、支付和流通；
- ◆ 集储蓄、信贷和非现金结算等多种功能为一体；
- ◆ 可广泛应用于生产、交换、分配和消费领域；
- ◆ 使用简便、安全、迅速、可靠；
- ◆ 电子支付通常要经过银行专用网络。

## 三、电子支付模式

### 1、信用卡支付方式

目前，基于信用卡的支付有四种类型：无安全措施工的信用卡支付、通过第三方代理人的支付、简单信用卡加密、SET信用卡方式。

- ◆ 无安全措施信用卡支付：买方通过网上从卖方订货，而信用卡信息通过电话、传真等非网上传送，或者信用卡信息在互联网上传送，但无任何安全措施，卖方与银行之间使用各自现有的银行商家专用网络授权来检查信用卡的真伪；
- ◆ 通过第三方代理人的支付：使卖方看不到买方信用卡信息，避免信用卡信息在网上多次公开传输而导致的信用卡信息被窃取。

- ◆ 简单加密信用卡支付：使用简单加密信用卡模式付费时，当信用卡信息被买方输入浏览器窗口或其他电子商务设备时，信用卡信息就被简单加密，安全地作为加密信息通过网络从买方向卖方传递。采用的加密协议有SHTTP、SSL等。

安全电子交易SET信用卡支付：订单和个人账号信息在Internet上安全传输，保证网上传输的数据不被黑客窃取；订单信息和个人账号信息的隔离。在将包括持卡人账号信息的订单送到卖方时，商家只能看到订货信息，而看不到持卡人的账户信息；持卡人和商家相互认证，以确定通信双方的身份。一般由第三方机构负责为在线通信方双方提供信用担保；要求软件遵循相同协议和消息格式，使不同厂家开发的软件具有兼容和互操作功能，并且可以运行在不同的硬件和操作系统下台上。

SET使用的安全技术有对称密钥系统、公钥系统、消息摘要、数字签名、数字信封、双重签名、认证等技术。前面已介绍过对称密钥系统、公钥系统、消息摘要、数字签名，下面介绍数字信封、双重签名和认证等。

## 2、数字现金支付方式

数字现金（E-cash）是一种表示现金的加密序列数，它可以用来表示现实中各种金额的币值。

## 3、电子支票支付方式

电子支票使得买方不必使用写在纸上的支票，而是用写在屏幕上的支票进行支付活动。

## 四、电子支付协议分类

目前对电子支付协议的分类方法有多种。

根据支付协议所包含的内容，把协议划分为“纯”支付协议（比如Modex，DigiCash）和综合支付协议（比如SET）；

根据支付时是否需要中介机构（比如电子银行）的参与，把支付协议划分为三方支付协议（SET）和两方支付协议（SSL，电子现金）；

根据传输方式，把支付协议划分为信用卡、借记卡、电子支票和电子现金等；

根据每笔交易的支付方式，把协议划分为按笔结算（使用信用卡和电子现金）和记帐方式（借记/货卡、订购）；

根据支付流传递的是指令还是电子货币，而将支付协议划分为两大类：类似于支付指令的支付系统和类似于数字货币转拨的支付系统。类似于支付指令的支付系统又可分为两种：1) 银行转拨2) 信用卡。信用卡协议是目前电子商务中使用最多的电子支付协议。

# 1、实际生活中使用信用卡购物的情景

- ◆ 持卡人在商场中浏览并选择商品
- ◆ 持卡人决定购买一些商品，如将有关商品放入购物小推车或购物篮之中
- ◆ 持卡人在商场的POS前，由POS机逐一确认所购物品，并自动打印购物清单、单价、总价和有关折扣等信息，交给持卡人消费者签名用来付款的信用卡

- ◆ 持卡人将选择付款，即指定要用来付款的信用卡
- ◆ 持卡人将信用卡交给POS刷卡
- ◆ 商户的POS将持卡人的帐号信息送到银行验证
- ◆ 商户接收POS机所打印的清单确认
- ◆ 商户按清单将货发给持卡人（可以当时提货或送货）

## 2、网上购物流程

- ◆ 持卡人使用浏览器去查看因特网上商户建立的购物中心主页上发布的商品；
- ◆ 持卡人决定购买一些商品，并加入购物篮；
- ◆ 持卡人从该商户站点上得到一个订货单，包括商品名称、单价、总额、提货方式等；

- ◆ 持卡人选择付款方式，即指定要用来付款的信用卡；
- ◆ 持卡人将订货单和付款指令发给商户（商户看不到付款指令）；
- ◆ 商户将持卡人的帐号信息送到持卡人开户银行验证；
- ◆ 商户接收订货合同；
- ◆ 商户接订单将货发给持卡人；
- ◆ 商户要求持卡人开户行将货款通过银行间清算网络付给它。

### 3、 在线支付过程：

通常，各个零售网站采用的方法是与国内的金融机构和电子货币专营企业进行合作。“由专业人来做专业事”，在线支付从一开始就属于金融机构的业务范围，那么从事电子商务的企业将网上支付的安全保障工作交由专业的在线安全服务公司。

具体的操作过程对于消费者来说其实十分简单，消费者在使用时既可以采用本地浏览器本身提供的安全机制，也可以直接在线利用银行提供的安全代理服务。所谓基于浏览器的安全机制，是指消费者根据自己所采用的浏览器类型，从网上下载对应的“CA根证书”，在系统的提示下获得浏览器本身提供的安全保障机能；而使用银行提供的安全代理机制，则可以使消费者得到由银行方面提供的加密安全保护。

这样一旦您输入了您的个人信息，并决定发送时，所有这些信息就会以高位数加密的方式，通过网络传递给发行信用卡或开设帐户的银行，由其确认并实施划帐服务，然后再把划帐成功的信息通知网站和正在网络上采购的您。到这时，您就只需要在家等着收货了。

可以看到其实在网上进行货币支付，在安全性方面其实远比一般的传统信用卡消费要安全许多。由于采用了高位加密的方式进行数据传输（例如对称加密、非对称密码算法等等），因此即便有人暗地截流了您传送的信息，在可以预计的未来要想破解这些信息，也是不大可能的。

# 第八节

## 电子商务主要的 安全要素

- 一、电子商务主要的安全要素
- 二、电子商务采用的主要安全技术及其标准规范

# 一、电子商务主要的安全要素：

考虑到安全服务各方面要求的技术方案已经研究出来了,安全服务可在网络上任何一处加以实施。但是,在两个贸易伙伴间进行的EC,安全服务通常是以"端到端"形式实施的(即不考虑通信网络及其节点上所实施的安全措施)。所实施安全的等级则是在均衡了潜在的安全危机、采取安全措施代价及要保护信息的价值等因素后确定的。这里将介绍EC应用过程中主要采用的几种安全技术及其相关标准规范。

# 1、加密技术

加密技术是EC采取的主要安全措施,贸易方可根据需要在信息交换的阶段使用。目前,加密技术分为两类,即对称加密和非对称加密。

# 对称加密/对称密钥加密/专用密钥加密

在对称加密方法中，对信息的加密和解密都使用相同的密钥。使用对称加密方法将简化加密的处理，每个贸易方都不必彼此研究和交换专用的加密算法，而是采用相同的加密算法并只交换共享的专用密钥。对称加密技术存在着在通信的贸易方之间确保密钥安全交换的问题。

此外，当某一贸易方有“n”个贸易关系，那么他就要维护“n”个专用密钥(即每把密钥对应一贸易方)。对称加密方式存在的另一个问题是无法鉴别贸易发起方或贸易最终方。因为贸易双方共享同一把专用密钥，贸易双方的任何信息都是通过这把密钥加密后传递给对方的。

数据加密标准(DES)由美国国家标准局提出,是目前广泛采用的对称加密方式之一,主要应用于银行业中的电子资金转帐(EFT)领域。DES的密钥长度为56位。三重DES是DES的一种变形。这种方法使用两个独立的56位密钥对交换的信息(如EDI数据)进行3次加密,从而使其有效密钥长度达到112位。

RC2和RC4方法是RSA数据安全公司的对称加密专利算法。RC2和RC4不同于DES,它们采用可变密钥长度的算法。通过规定不同的密钥长度,RC2和RC4能够提高或降低安全的程度。一些电子邮件产品(如Lotus Notes和Apple的Opn Collaboration Environment)已采用了这些算法。

## 非对称加密/公开密钥加密

在非对称加密体系中，密钥被分解为一对(即一把公开密钥或加密密钥和一把专用密钥或解密密钥)。这对密钥中的任何一把都可作为公开密钥(加密密钥)通过非保密方式向他人公开，而另一把则作为专用密钥(解密密钥)加以保存。公开密钥用于对机密性的加密，专用密钥则用于对加密信息的解密。专用密钥只能由生成密钥对的贸易方掌握，公开密钥可广泛发布，但它只对应于生成该密钥的贸易方。

贸易方利用该方案实现机密信息交换的基本过程是：贸易方甲生成一对密钥并将其中的一把作为公开密钥向其他贸易方公开；得到该公开密钥的贸易方乙使用该密钥对机密信息进行加密后再发送给贸易方甲；贸易方甲再用自己保存的另一把专用密钥对加密后的信息进行解密。贸易方甲只能用其专用密钥解密由其公开密钥加密后的任何信息。

RSA(即Rivest, Shamir Adleman)算法是非对称加密领域内最为著名的算法,但是它存在的主要问题是算法的运算速度较慢。因此,在实际的应用中通常不采用这一算法对信息量大的信息(如大的EDI交易)进行加密。对于加密量大的应用,公开密钥加密算法通常用于对称加密方法密钥的加密。

## 2、密钥管理技术

### 对称密钥管理

对称加密是基于共同保守秘密来实现的。采用对称加密技术的贸易双方必须要保证采用的是相同的密钥,要保证彼此密钥的交换是安全可靠的,同时还要设定防止密钥泄密和更改密钥的程序。这样,对称密钥的管理和分发工作将变成一件潜在危险的和繁琐的过程。

通过公开密钥加密技术实现对称密钥的管理使相应的管理变得简单和更加安全,同时还解决了纯对称密钥模式中存在的可靠性和鉴别问题。

贸易方可以为每次交换的信息(如每次的EDI交换)生成唯一一把对称密钥并用公开密钥对该密钥进行加密,然后再将加密后的密钥和用该密钥加密的信息(如EDI交换)一起发送给相应的贸易方。

由于对每次信息交换都对应生成了唯一一把密钥,因此各贸易方就不再需要对密钥进行维护和担心密钥的泄露或过期。这种方式的另一优点是即使泄露了一把密钥也只将影响一笔交易,而不会影响到贸易双方之间所有的交易关系。这种方式还提供了贸易伙伴间发布对称密钥的一种安全途径。

## 公开密钥管理/数字证书

贸易伙伴间可以使用数字证书(公开密钥证书)来交换公开密钥。国际电信联盟(ITU)制定的标准X.509(即信息技术--开放系统互连--目录:鉴别框架)对数字证书进行了定义该标准等同于国际标准化组织(ISO)与国际电工委员会(IEC)联合发布的ISO/IEC 9594-8:195标准。

数字证书通常包含有唯一标识证书所有者(即贸易方)的名称、唯一标识证书发布者的名称、证书所有者的公开密钥、证书发布者的数字签名、证书的有效期及证书的序列号等。证书发布者一般称为证书管理机构(CA),它是贸易各方都信赖的机构。数字证书能够起到标识贸易方的作用,是目前EC广泛采用的技术之一。微软公司的Internet Explorer 3.0和网景公司的Navigator 3.0都提供了数字证书的功能来作为身份鉴别的手段。

# 密钥管理相关的标准规范

前国际有关的标准化机构都着手制定关于密钥管理的技术标准规范。ISO与IEC下属的信息技术委员会(JTC1)已起草了关于密钥管理的国际标准规范。该规范主要由3部分组成:第1部分是密钥管理框架;第2部分是采用对称技术的机制;第3部分是采用非对称技术的机制。该规范现已进入到国际标准草案表决阶段,并将很快成为正式的国际标准。

### 3、数字签名

数字签名是公开密钥加密技术的另一类应用。它的主要方式是:报文的发送方从报文文本中生成一个128位的散列值(或报文摘要)。发送方用自己的专用密钥对这个散列值进行加密来形成发送方的数字签名。然后,这个数字签名将作为报文的附件和报文一起发送给报文的接收方。

报文的接收方首先从接收到的原始报文中计算出128位的散列值(或报文摘要),接着再用发送方的公开密钥来对报文附加的数字签名进行解密。如果两个散列值相同,那么接收方就能确认该数字签名是发送方的。通过数字签名能够实现对原始报文的鉴别和不可抵赖性。

ISO/IEC JTC1已在起草有关的国际标准规范。该标准的初步题目是"信息技术安全技术带附件的数字签名方案",它由概述和基于身份的机制两部分构成。

## 4、Internet电子邮件的安全协议

电子邮件是Internet上主要的信息传输手段,也是EC应用的主要途径之一。但它并不具备很强的安全防范措施。Internet工程任务组(IEFT)为扩充电子邮件的安全性能已起草了相关的规范。

PEM是增强Internet电子邮件隐秘性的标准草案,它在Internet电子邮件的标准格式上增加了加密、鉴别和密钥管理的功能,允许使用公开密钥和专用密钥的加密方式,并能够支持多种加密工具。PEM是通过Internet传输安全性商务邮件的非正式标准。PEM有可能被S/MIME和PEM-MIME规范所取代。

S/MIME(安全的多功能Internet电子邮件扩充)是在RFC1521所描述的多功能Internet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。MIME是正式的Internet电子邮件扩充标准格式,但它未提供任何的安全服务功能。S/MIME的目的是在MIME上定义安全服务措施的实施方式。S/MIME已成为产界业广泛认可的协议,如微软公司、Netscape公司、Nov11公司、Lotus公司等都支持该协议。

。

PEM-MIME(MOSS)(MIME对象  
安全服务)是将PEM和MIME两者的  
特性进行了结合。

## 5、Internet主要的安全协议

SSL(安全槽层)协议是由Netscape公司研究制定的安全协议,该协议向基于TCP/IP的客户/服务器应用程序提供了客户端和服务器的鉴别、数据完整性及信息机密性等安全措施。该协议通过在应用程序进行数据交换前交换SSL初始握手信息来实现有关安全特性的审查。

在SSL握手信息中采用了DES、MD5等加密技术来实现机密性和数据完整性,并采用X.509的数字证书实现鉴别。该协议已成为事实上的工业标准,并被广泛应用于Internet和Intranet的服务器产品和客户端产品中。如Netscape公司、微软公司、IBM公司等领导Internet/Intranet网络产品的公司已在使用该协议。

S-HTTP(安全的超文本传输协议)是对HTTP扩充安全特性、增加了报文的安全性,它是基于SSL技术的。该协议向WWW的应用提供完整性、鉴别、不可抵赖性及机密性等安全措施。目前,该协议正由Internet工程任务组起草RFC草案。

## 6、UN/EDIFACT的安全

UN/EDIFACT报文是唯一的国际通用的EDI标准。UN/EDIFACT的安全措施主要是通过集成式和分离式两种途径来实现。集成式的途径是通过在UN/EDIFACT报文结构中使用可选择的安全头段和安全尾段来保证报文内容的完整性、报文来源的鉴别和不可抵赖性；而分离式途径则是通过发送3种特殊的UN/EDIFACT报文(即AU TCK、KEYMAN和CIPHER来达到保障安全的目的。

## 7、安全电子交易规范(SET)

SET向基于信用卡进行电子化交易的应用提供了实现安全措施的规则。它是由Visa国际组织和万事达组织共同制定的一个能保证通过开放网络(包括Internet)进行安全资金支付的技术标准。SET主要由3个文件组成,分别是SET业务描述、SET程序员指南和SET协议描述。SET 1.0版已经公布并可应用于任何银行支付服务。

上述介绍的技术及其标准规范是EC应用中主要涉及的技术，还有很多安全技术及标准规范尚未列出。要保证EC安全可靠，首先要明确EC的安全隐患、安全等级和采用安全措施的成本，再选择相应的安全措施。EC应用的安全方案已逐步形成，EC时代即将到来。

THANK YOU

