

# 电子签章 / 签名——网络时代的身份证

许兆然 博士

## 一、应用背景

随着我国政府信息化的层层推进,对电子印章应用需求的呼声越来越高,对电子印章的安全性也越来越重视,印章是来代表政府、企业的权威及法人资格和个人的信用,印章是公文生效的重要标志。没有盖章的公文缺乏权威象征。

互联网已经慢慢地渗透到我们的日常生活中,从各个方面不经意地改变着人类的生活。电子商务越来越接近理想中的样子了;电子政务也正在一步步地走向我们……这一系列新兴网络行业发展的同时也带来了许多法律问题,如网络通讯的安全与隐私保护问题、知识产权问题、电子支付问题、合同问题、交易认证问题等等,电子签名制度问题也是其中一个重要方面。为此,国家经过广泛的征求意见和修改,出台了《中华人民共和国电子签名法》,在2005年4月1日已正式启用,其中:

### 第三章 电子签名与认证

第十四条 可靠的电子签名与手写签名或者盖章具有同等的法律效力。

公安部有关负责人说,电子印章是我国印章史上的一场革命。电子印章管理应用系统将世界上先进的数字认证技术应用于印章治安管理,强化对电子印章的制作和应用各个环节的管理,确保电子印章持有者身份真实可靠。

下面我们就来了解一下有关问题。

为什么要采用电子签章?

传统的政府间的公文传送和交易行为,必须要用书面的文件来完成,为了保证文件是某个当事人或者机关签发的,并且文件没有被篡改,还必须要有签发人的手写签字或者公章。

网络环境中,文件的传递采取电子的方式,比如E-mail。这种方式最大的优点就是速度快,文件可以

在数秒中到达远在万里之外的客户手中。在“时间就是金钱、效率就是生命”的生意场上,这种优势无疑成为广大厂商的首选。

电子文件并非只用于政府文件的传递和合同的签订,而是适用于所有信息的传递。可以理想化地认为,未来的信息传递,可以不借助于任何纸张。

如何保证一项文件或者一条信息是某个人发出的?某个人发出文件或者信息后,如果发现对自己不利抵赖怎么办?如果文件或者信息在网络传输过程中被他人截取,并被修改了怎么办?许多人都知道,我们平时发送和接收的电子邮件是不加密的,对于某些人比如网管员来说,看这些文件甚至比看没有封上的书面信件更容易。

电子签章就是用于电子文件之上,与传统的手写签名、盖章具有完全相同功能的技术。有了电子签章,任何信息都可以放心地通过网络以电子文件的形式传输,因此,电子签章问题是电子政务和电子商务建设中必须首先解决的核心问题。

## 二、应用现状

### 1、主要技术

#### 1) 电子签章的原理

电子签章泛指所有以电子形式存在,依附在电子文件并与其逻辑相关,可用以辨识电子文件签署者身份,保证文件的完整性,并表示签署者同意电子文件所陈述事项的内容。包括数字签章技术和逐渐普及的用于身份验证的生物识别技术如指纹、面纹、DNA技术等。

目前最成熟的电子签章技术就是“数字签章(Digital Signature)”,它是以公钥及密钥的“非对称型”密码技术制作的电子印章。使用原理大致为:由计算机程序将密钥和需传送的文件浓缩成

信息摘要予以运算，得出数字签章，将数字签章并同原交易信息传送给交易对方，后者可用来验证该信息确实由前者传送、查验文件在传送过程是否遭他人篡改，并防止对方抵赖。由于数字签章技术采用的是单向不可逆运算方式，要想对其破解，以目前的计算机速度至少需要1万年以上，几乎是不可能的。文件传输是以乱码的形式显示的，他人无法阅读或篡改。因此，从某种意义上讲，使用电子文件和数字签章，甚至比使用经过签字盖章的书面文件安全得多。

## 2) 主要技术及特点

### ① PKI/PMI 技术

运用公钥密码体制构建公钥基础设施PKI，是在大型开放网络环境下解决信息安全问题的可行、有效的方法。公开密钥基础设施的目的是管理密钥和证书。通过PKI对密钥和证书的管理，可以创建和维护一种可信的网络环境。PKI使得密码技术和数字签名技术可以用于各种应用环境。公钥基础设施PKI是国家信息安全建设中极其关键的基础性设施，它在底层网络基础设施的基础上提供了一个一致的信息安全服务层面，弥补了网络基础设施与用户应用在安全需求方面的差异。

电子政务系统采用PKI/PMI技术，可得到全网统一的签名、认证和授权服务。

PKI构成所谓的PKI安全平台，可提供智能化的信任服务；PMI构成所谓的特权管理平台，在PKI信息安全平台的基础上提供有效授权服务。

对于电子商务来说，最受关注的安全问题是信任和公正问题；而在政府办公计算机网络系统面临的一个重要且迫切需要解决的安全问题就是信息保密和访问权限控制。政府计算机网办公系统可以采用PKI技术来实现身份认证、访问权限控制和信息加密，尽管与电子商务PKI技术相类似，但在安全核心的体现上有着很大差别。

### ② USB Key 或指纹技术

电子签章系统中的指纹验证和识别是通过专门的指纹签名器来实现。指纹签名器的作用有两点：

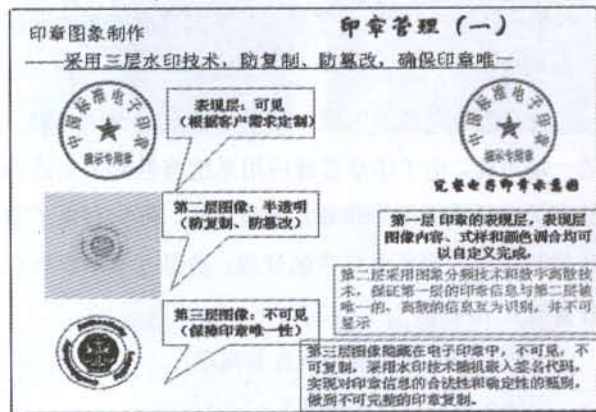
1. 存储用户数据：将一些重要数据如用户名、指纹信息等存储到指纹签名器中，用户使用这些数据时通过指纹验证，读出这些数据。

2. 存储用户私钥，并使用专门的CSP算法进行数字签名：在安装CA证书的时候，将证书的私钥存储到指纹签名器中。等到需要进行数字签名的时候，通过指纹验证将私钥取出，进行数字签名。

指纹验证识别有以下技术特点：智能图像处理、智能特征抽取、旋转不变性及平移不变性、模式特征点线结合，匹配准确度高、模糊快速搜索功能、智能神经网络、定点运算和嵌入式操作系统等。

### ③ 数字水印技术

电子签章使用数字水印和数字签名技术实现传统物理签章的同样功能，是签章文件具备和物理签章同样的法理基础，为政府公文来往、单位法律文件交换和私人法律与金融来往提供便捷、安全的现代信息手段。电子签章使用三层图像技术，如下图所示：



图：电子印章的三层水印技术

技术特点：

采用三层水印技术，具有防复制、防篡改，确保印章唯一功能。

基于CA体系，按照客户身份证及系统权限订做发放。

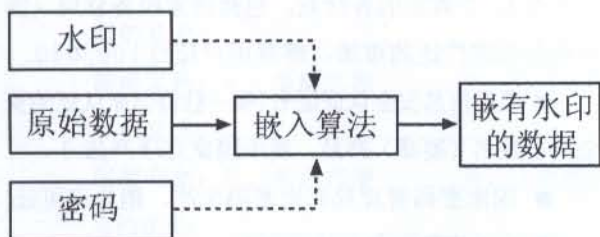
印章不仅本身为三层结构，不可复制和篡改，在签章的过程中，其底层的数字水印已经对公文整体进行了数字签名与水印包装，因此做到了对公文本身的防复制、防篡改。实现了签章与介质（公函）一体唯一性。

**永久性（鲁棒性）：**水印一旦被嵌入，数字水印将随原始数据一直存在，不因数据的某种改动而导致水印丢失，如图像文件的JPEG压缩和一般的图像处理过程。

**数据一致性：**嵌入数字水印的图像、视频、声音等原信息保持了极高的数据一致完整性，而隐蔽的数字水印难以被检测出来。

#### 数字水印系统模型

水印嵌入模型如下：



图：水印嵌入模型

#### 2、应用领域

随着我国《电子签名法》的实施，并结合成熟的数字签名技术，电子签章已逐步、广泛地应用到各行各业中。

##### 政府机关

政府机构内部的办公自动化、政府机关之间的收发文管理和联网办公需要相应的领导签名和电子印章，以保证电子公文等信息的完整性、防篡改性和不可抵赖性。安全、合法的电子签章系统既保证了政府公务的高效率，又利用现代化手段节约了能源，每年可省下大量的纸质成本，某地市一年就公文流转一项就比上年省下了数十万元。

##### 政府与企业

政府与企业之间存在大量的信息交换，如何确保

信息的安全是政府机关通过网上办公提高办事效率和服务水平的关键所在，利用安全、合法的电子签章技术可以从技术的可靠性和法律的有效性等方面确保了网上办公的安全性。如网上报税、网上申报、网上审批、网上工商年检、电子海关等应用。

##### 企业内部

电子签章广泛应用于企业或企业集团内部的协同办公、集团公司上下级单位之间的协同办公。为企业的网上协同办公提供了安全保证。如文件交换、财务报表、销售报表、物流管理等均需要电子签章。可以应用于各行各业，如制造业、商业、金融、电信、电力、建筑等行业。

##### 企业与企业

企业与企业之间的协同商务需要可信任的认证来保证信息交换的安全性和有效性。电子签章系统很好地解决了这一问题，如网上定单、物流数据交换、电子合同管理等等。

总之，在电子文件交换或电子交易过程中，凡是需要签字/盖章、确认身份的地方，就需要电子印章。

#### 3、主要作用及特点

在电子政务和电子商务活动中会有大量的文件需要流转，一般的纸质公文依靠印章、签名保证文档的有效性和完整性。如何为电子文档提供有效性、完整性保证呢？基于这样的思路，提出了“电子印章”的概念。电子印章的安全应用，加上“文档只读保护”设置便可杜绝印章伪造、移动、拷贝，从而有力保证文档的有效性。

电子签章系统应该具有以下特点：

★ 电子签章系统应该符合《中华人民共和国电子签名法》的相关要求；

★ 电子签章系统应该达到国家信息安全技术标准：GB/T18336-2001《信息技术 安全技术 信息技术安全性评估准则》和GB/T17903-1999《信息技术 安全技术 抗抵赖》；

★ 公章文件加密存储，只有得到公章管理员的授权方可使用公章；

★ 公文盖章或签字后，不允许修改；否则自动显示“文档已被更改”的字样；

★ 印章应该具备防复制、防拷贝、防篡改等功能

★ 公文的存储和传输都经过加密；

★ 用户可以验证公章文件的真假(包括本地验证、在线验证)；

★ 只有合法用户可以阅读公文；

★ 签章信息的验证。比如：签章时间、签章人、印章信息等；

### 三、应用趋势

电子签章/电子签名技术为中国各行各业以及企业的信息化提供了强有力的辅助手段。比如，目前中国已经投身于全球性的交流与竞争。如何增强政府职能部门的办事效率？如何在中西方之间顺利地进行政治、经济、文化的交流和贸易往来？显然，这需要电子政务和电子商务系统提供方便、快捷、安全的手段。而这些系统的完善离不开电子签名技术。

以最典型的办公自动化应用为例，电子签章/签名认证功能保证了公文和领导签名内容的不可更改性和来源的真实性。用户可以利用动态电子签章/签名认证实现可靠的身份确认功效，比传统的键盘密码更安全、更有效。用动态签名认证来替代传统密码口令验证，极大地增加了系统中信息的安全性，而且使用更加方便、容易。

而含有电子签章/签名技术的办公自动化系统则可以大大减少重复劳动，使各个部门、各个环节的单独处理工作串联起来，同时也能处理流程上多个环节的任务。除了可以方便进行各个环节的审核、批复、签字，同时也可以进行不同环节批复的查询。它不仅解决了传统办公的效率低下和纸张浪费状况，而且也解决了因领导无法使用繁琐的现代办公自动化系统而闲置的巨额信息化投资。

实践证明，电子签章/签名技术越来越受到众多

用户的青睐，因为他们可享受最自然、最人性化的便利技术。这些应用遍布于各级政府的电子政务系统、金融领域的安全信用应用系统、企业信息化的众多应用、军队的政令传达、CAD/CAM领域的设计流程应用、医疗移动临床系统和院校的远程教育系统等诸多领域。

### 四、关于百成

百成科技集团 (PREVAIL INTERNATIONAL LTD.) 是2005年11月成立于BVI (BRITISH VIRGIN ISLAND) 的海外公司，控股广州市百成科技有限公司 (简称“广州百成”) 和香港 ANTELCOMMUNICATION COMPANY LTD. (简称“ANTEL”)。是一个形成技术研发、产品生产、市场运作的大型集团化企业。主营业务为电子签名和电子交易的安全服务，在中国大陆具有15个省市的各行业，包括国家税务总局、国家商务部等广泛的市场，终端用户超过100,000。

■ 国家信息安全认证证书(唯一获得国家认证的安全电子签名(签章)产品，属于国家立项产品)

■ 国家密码管理局商用密码生产、销售许可证

■ 广东省软件企业认定证书

■ 国家科技部立项证书

■ 国家科技部/广州市科技局立项/鉴定，科技进步奖一等奖证书

■ 首家获得香港资讯科技基金(ITF)——粤港合作项目奖

■ 唯一获得微软中国技术中心完成百成电子印章兼容性测试 [http://www.microsoft.com/china/CTC/Newsletter/newsletter200506/successful\\_case.htm](http://www.microsoft.com/china/CTC/Newsletter/newsletter200506/successful_case.htm)

