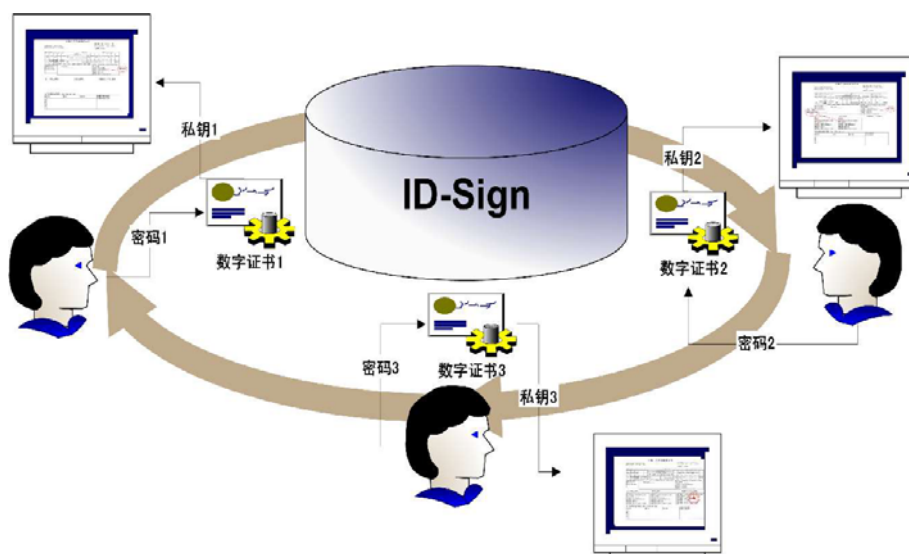


# 多层次Web数字签章应用软件

## ID-Sign for Web

### 1、综述

龙方自主研发的基于Web 的数字签章应用软件，ID-Sign for Web 旨在帮助组织机构从一个手工操作的、低效率的书面处理过程迁移到一个自动化的、全面集成的、高度安全的流水线作业。ID-Sign for Web 是基于Web 的签名控件，可以嵌入任何Web 表格或文档中，提供签名、盖章、验证的功能。通过普通的IE、Mozilla 等浏览器完成对敏感数据的签名保护，不需要在客户端安装应用程序。企业用户和政府职员可以直接使用ID-Sign，和现有的办公软件无缝的配套工作，真正实现无纸化办公。企事业单位和信息化解决方案提供商利用它，可以在不改变原有的IT 系统情况下，极为方便地建立适合各种需求的安全、可靠的信息化应用软件系统。



图A1 ID-Sign 促进办公自动化。

### 2、ID-Sign for Web 介绍

ID-Sign for Web 与其他签名产品相比，创新之处在于它能支持多方连署或会签，也就是说允许多人针对一个文档中不同的域、段落、页面分别签名，而且签名和文档内容的完整性是可验证的。这个功能在多层审批、多方合同签订等领域用途非常广泛。

ID-Sign for Web 支持软件签名和硬件签名两种方式。龙方公司同国内前5 大生产USB KEY 的公司及上海CA、山东CA 建立了战略合作关系。用任何一家生产的key 或证书都可以在龙方签名平台上完成软硬件签名。

## ID-Sign for Web Datasheet:

特点	ID-Sign for Web
联署会签	支持，一个表格中支持多方多次签名与加盖印章。
功能及组成	基于web 网页的插件软件。用IE 或Mozilla 在线浏览、填表、签名和验证。
WYSWYG 表格设计器	有。如果用XML 表格，可以用ID-FormDesigner 表格设计器，如果用普通网页表格，任何网页设计器都可以。
支持的浏览器	IE、Mozilla firefox
印章显示	有，印章和签名都及时显示在浏览器的页面上。
Web 页面格式	可以与JSP 或ASP 或PHP 开发的Web 系统集成
硬件USB Key	支持
查看证书信息	支持
个人证书与密钥管理	有
时间戳	有
国际化	简体中文，英文

## 2.1 功能结构及组成

ID-Sign for Web 是一个完整的数字签章应用软件，提供了丰富的应用工具和签名工具。ID-Sign for Web 通过基于web 浏览器的Java Applet 控件，提供在IE 、Mozilla 浏览器里面的文件（文本或表格）进行签名、加盖印章、验证内容和认证签名人身份等的功能。所有的工具也都采用自动化管理和自行管理相结合的方式，灵活易用，方便管理。

## 2.2 技术特点和优势

### 2.2.1 多方联署、会签，提高效率

在公文流转过程中，尤其是网上交易、网上采购、网上招投标中涉及的各种文件，都需要不只一方的签名和印章。ID-Sign 的最具创新之处在于它支持多方连署或会签，也就是说允许多人针对一个文档中不同的域、段落、页面分别签名，而且签名和文档内容的完整性是可验证的。也因为这个特点，系统支持追加批语，每个签名都可以独立验证。

### 2.2.2 数字签名完全遵循国际标准

ID-Sign 是完全遵循PKCS 、X.509 v.3 标准、及与多种机构的证书兼容，可交叉验证。目前支持上海CA 的证书、飞天诚信、明华、华虹、大明五洲等的密钥锁。

### 2.2.3 电子水印章

ID-Sign 带有电子水印章的功能，提供信息的完整性的保障。虽然印章看似一个图片，但是，它里面经过算法的处理，已经将被盖章的数据值、数字签名值等内容嵌入到印章的图案中，可验证印章的有效性。也就是说，如果印章只是简单的图片而不是与文件的内容绑定为一体的话，就能提醒接收方这个章是否是被授权者加盖的，提供信息完整性与不可抵赖性保障。

#### 2.2.4 本地或联网验证

ID-Sign 支持本地或联网验证。除了内容完整性验证以外，可验证证书的有效期、废除列表、证书颁发机构等内容。而且一旦数字签名验证不通过，印章图片会显示灰色横线以示用户签名已经失效。

#### 2.2.5 采用Java 语言，跨平台、跨软件操作

ID-Sign for Web 均采用JAVA 语言，所以可以支持多种操作系统，包括Windows 、Linux 、Unix，跨平台使用。

#### 2.2.6 数据与显示分离

数据与显示分离的好处还在于表格里面的数据可以被容易的重复使用及调用，避免了重复输入的麻烦。

#### 2.2.7 个人密钥和证书管理

由于ID-Sign 数字签名默认采用PKI 技术，所以就要有配套的个人密钥和证书的管理机制，或用第三方证书机构的证书和管理工具，只要他们的产品遵循国际x509 v3 标准。ID-Sign 提供的管理功能包括以下几个方面：

- 自动化管理（生成、导入、导出等）个人密钥和证书。
- 自动验证和确认密钥和证书。
- 支持多种密钥和证书存储模式，包括在本地PC 中加密存储、加密锁或加密卡等。
- 支持一人多密钥多证书
- 可支持USB 密钥库
- 支持任何遵循X.509v3 规范的证书
- 支持多种密钥库格式，包括PKCS12 、JKS、UBER 、PKCS11

#### 2.2.8 与龙方的安全中间件无缝集成

签名和印章在物理空间中是严格管理的，我们也为电子空间提供了一个强大的管理机制，叫做ID-Enterprise，安全中间件。它提供一套整合式的安全政策管理机制，其功能包括安全审计记录、系统时间戳、细粒度的角色与用户的权限分配等，尤其是对印章与签名的管理，杜绝越权操作。

### 3. ID-Sign for Web 签名演示说明

截图一说明：上面是一张加载了龙方签名控件的网页。在签名的地方有两个按钮，写有“签名”和“验证”，分别用来完成对页面内容的签名和对签名的验证。

截图二说明：用鼠标左点击网页上“签字”右边横线上方，签名控件就会把同这个签名绑定的输入框用红色的框勾勒出来。让签名的人一看就知道，他的这个签名签的是哪些内容，也就是他需要对这些输入框里的内容负责。



截图三说明：点击“签名”按钮，会弹出一个对话框，要求定位证书库的位置。这种签名方式是软件签名。如果是硬件签名方式，就要把签名的key 插到计算机的USB 口中，对话框中会显示key 中证书库的信息。



截图四说明：从硬盘上选择自己的证书库，输入正确的证书库密码，点击“确定”按钮，龙方签名控件就会完成对网页上锁定的内容的签名。



截图五说明：在完成签名后，在签名的位置上就会出现签名者的信息，签名的时间及一个图形形式的印章。

截图六说明：在签名后，点击“验证”按钮就可以验证签名的有效性。点击按钮的同时，签名控件会把同这个签名关联的内容用红色的框标识出来。验证的时候一眼就看出这个签名签的是哪些内容。如果锁定的内容没有修改，就会弹出对话框显示“签名有效”字样，同时显示签名者使用的证书库的信息。



截图七说明：如果修改了签名锁定的内容，比方在“帐户序号”里添加一些字母。再去验证签名，这时候签名锁定的内容被修改了。签名控件就会弹出个对话框，显示“签名无效”字样，同时，签名者的签字处会出现一条红色的线，告诉验证的人，内容被篡改了。

## 4、应用范围

ID-Sign for Web 是一个完整的数字签名与印章的应用软件产品。适用于各级政府机关、事业单位和各型企业中的电子政务、电子商务、网上交易平台、协作平台。多步、多层、在线或离线审批、签名流程管理等方面。特别对有大量的行政文书工作、公文表格处理的事务密集的大型企事业单位和政府机构，龙方的产品让他们真正实现可灵活配置的无纸化办公，同时，营造一个安全的网上工作环境，为他们带来巨大的成本和管理效益。图A4、ID-Sign 应用软件适用于广泛的应用领域、操作系统及硬件环境中。

