电子印章服务器白皮书

（版本：3.2）

中金国信

2016年7月27日

版权声明：本文档的版权属于北京中金国信科技有限公司，任何人或组织未经许可，不得擅自修改、拷贝或以其它方式使用本文档中的内容。

**文档修订记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **内容** | **日期** | **编写** | **审核** |
| 1.0 | 初稿 | 2014/7/15 | 芮元生 |  |
| 2.0 | 第二版 | 2015/5/26 | 程智宝 |  |
| 3.2 | 添加新模块功能 | 2016/7/27 | 王亮洁 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目 录**

[1 产品背景 3](#_Toc457391008)

[2 总体介绍 4](#_Toc457391009)

[3系统模块 4](#_Toc457391010)

[3.1总体架构 4](#_Toc457391011)

[3.2 系统流程 5](#_Toc457391012)

[3.3主要模块 6](#_Toc457391013)

[3.3.1机构管理 6](#_Toc457391014)

[3.3.2管理员管理 6](#_Toc457391015)

[3.3.3印模管理 6](#_Toc457391016)

[3.3.4印章管理 6](#_Toc457391017)

[3.3.5 签章管理 7](#_Toc457391018)

[3.3.6有效性验证管理 8](#_Toc457391019)

[3.3.7用户管理 8](#_Toc457391020)

[3.3.8日志管理 8](#_Toc457391021)

[3.3.9系统管理 8](#_Toc457391022)

[4技术实现 8](#_Toc457391023)

[4.1 签名规范 8](#_Toc457391024)

[5名词解释 9](#_Toc457391025)

# 

# 1 产品背景

随着互联网的发展，对电子化办公的需求越来越强烈，传统的纸质签字盖章行为，由于成本高、效率低下、不环保等缺点，渐渐会被更节能环保、高效的电子化行为所代替，如电子回单、电子收单、电子发票等一系列有电子化签字盖章的行为。成熟可靠的数字签名技术结合传统的电子图片，呈现给人一种所见即所得的电子印章，是未来发展的必然趋势。

特别的随着电子政务的深入发展和《中华人民共和国电子签名法》的颁布和实施，实现在电子公文中加盖电子印章已成为企事业数字化无纸办公的必需功能。

电子印章服务器系统的建设旨在结合CA数字认证技术，建立一套安全、实用，并为国家认可的电子印章系统，以统一的电子公文版式和电子印章，完美实现电子政务的无纸化办公，提高办公效率的目标。

# 2 总体介绍

电子印章服务器是一整套电子签章验章解决方案，采用电子签名技术在电子文档和WEB页面上实现电子印章签章及验章功能。

印章服务器包括印模管理、印章管理、印章制作、PDF签章和WEB签章，并且提供了完整的制章、签章和验章的接口以便调用。

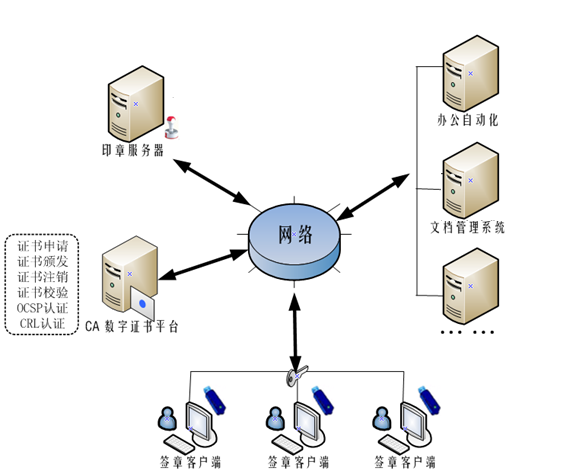
电子印章服务器可以单独使用实现电子印章功能，也可以调用服务器提供的接口更好的整合到现有的软件平台中。

# 3系统模块

## 3.1总体架构

电子印章服务器端现有印模管理、印章管理、签章管理、有效性验证管理等九大模块，并提供完整的制章、签章和验章的接口，能够被各类应用系统无缝集成，如OA 系统、ERP 系统、财务系统、档案管理系统、合同管理平台、邮件系统、短信系统、供应链系统等。

## 3.2 系统流程



印章服务器本身提供了印模管理、印章管理、印章制作、PDF签章、WEB签章功能，用户可以上传图片和密钥进行制章操作，服务器会根据特定的结构进行保存；同时用户也可以上传PDF文件或者直接输入原文进行PDF签章或WEB签章验章。

用户也可以根据服务器提供的接口（详见电子印章服务器接口文档（3.2）.docx）进行制章、签章和验章操作。

## 3.3主要模块

电子印章服务器端现有机构管理、管理员管理、印模管理、印章管理、签章管理、有效性验证管理、用户管理、日志管理、系统管理九大模块。

### 3.3.1机构管理

机构管理模块的主要功能是印章机构管理，默认机构是“根机构”，可添加新的机构，可对机构进行编辑和删除，“根机构”建议保留。

### 3.3.2管理员管理

管理员管理模块的主要功能是对电子印章服务器端操作人员管理，默认机构是“超级管理员”，对管理员可添加、编辑。

### 3.3.3印模管理

印模管理模块的主要功能是制模管理，制模包括手工制模、自动制模、同心圆印模、印模管理，主要功能是根据上传的图片和印模信息或者印章图片相关数据信息制作电子印模，并上传到服务器，保存到数据库，由服务器端统一对制作的印模进行管理。

### 3.3.4印章管理

印章管理模块的主要功能是制章管理、印章管理、印章证书管理，制章主要功能是选择的印模和PFX或者选择服务器证书制作电子印章保存到服务器，并由服务器对印章进行管理。证书管理主要是在服务器生成软硬件证书，以供制作电子印章时使用。

### 3.3.5 签章管理

签章管理是对印章的实际应用，目前主要分为PDF签章和WEB签章。PDF签章是对PDF文件进行盖章操作，而WEB签章主要是对HTML端原文进行签章、验章操作。

PDF签章是对PDF文件进行盖章操作，选择将要进行签章操作的PDF文件，选择进行签章的印章（印章编码\_印章名称），选择签章规则（包括空白标签处盖章、位置盖章、关键字盖章）。关键字盖章需要输入关键字，位置盖章需要输入页码、坐标等信息。

PDF签章效果图：



WEB签章用于web端的电子签章及验章， 选择用于签章的印章、印章密码、本次签章地点及原因、输入待签章内容，然后点击签章，即可生成签章结果。

### 3.3.6有效性验证管理

有效性验证管理模块的主要功能是设置验证证书有效性的信息，包括证书链管理、CRL管理，系统默认信任CFCA颁发的证书，将CFCA根证作为信任证书，管理CRL列表，可上传和删除该列表。

### 3.3.7用户管理

用户管理模块的主要功能是使用印章的用户管理，对使用系统印章的用户信息进行维护，可添加、编辑、删除用户。

### 3.3.8日志管理

日志管理模块的主要功能是实现对用户操作日志的查询、归档操作的记录。

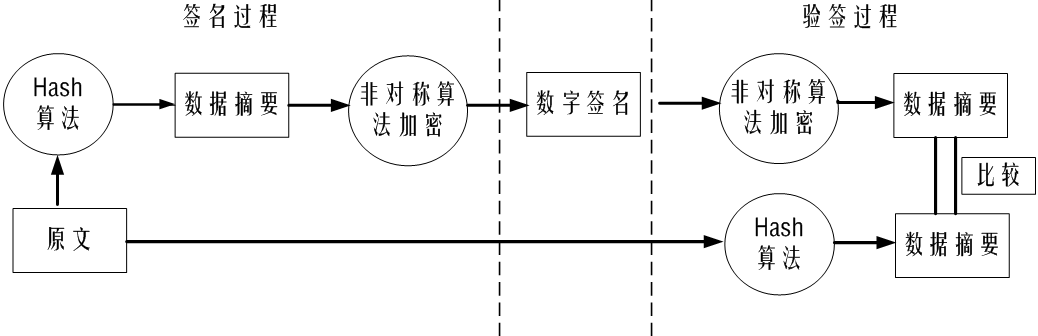
### 3.3.9系统管理

系统管理模块的主要功能是实现管理员修改密码的功能。

# 4技术实现

## 4.1 签名规范

数字签名的全过程分两大部分，即签名与验证。数字签名与验证的过程和技术实现的原理如下图:



左侧为签名，右侧为验证过程。即发方将原文用哈希算法求得数字摘要，用签名私钥对数字摘要加密得数字签名，发方将原文与数字签名一起发送给接受方；收方验证签名，即用发方公钥解密数字签名，得出数字摘要；收方将原文采用同样哈希算法又得一新的数字摘要，将两个数字摘要进行比较，如果二者匹配，说明经数字签名的电子文件传输成功。

# 5名词解释

**电子印章** 是电子签名一种表现形式，利用图像处理技术将电子签名操作转化为与纸质文件盖章操作相同的可视效果，同时利用电子签名技术保障电子信息的真实性和完整性以及签名人的不可否认性。

**数字证书** 数字证书也称电子证书（以下简称证书），是一种由特定机构（CA）数字签名的、包含公开密钥以及公开密钥拥有者信息的电子文档。如同现实生活中公安机关颁发的居民身份证一样，数字证书是网络环境中的一种身份证，用于证明某一实体（如人、服务器等）的身份。

**数字签名** 在进行数字签名过程中，发信者使用自己的私钥，通过非对称密码算法，对待发送数据的数字摘要（哈希值）进行加密，从而得到一段信息称为数字签名（Sign）。

**数字信封** 所谓数字信封就是信息发送端用接收端的公钥，将一个对称通信密钥进行加密，形成的数据称为数字信封。此数字信封传送给接收端，只有指定的接收方才能用自己的私钥打开数字信封，获取该对称密钥，于是，接收方可以用以解读传送来的密码通信信息。这就好比在生活中，将一把钥匙装在信封中，邮寄给对方，对方收到信件后，将钥匙取出，用它打开保险箱的道理一样。

**证书吊销列表（CRL）** 证书吊销列表CRL是一种包含吊销的证书列表的签名数据结构。CRL是证书吊销状态的公布形式，CRL就像信用卡的黑名单，它通知其他证书订户某些电子证书不再有效。