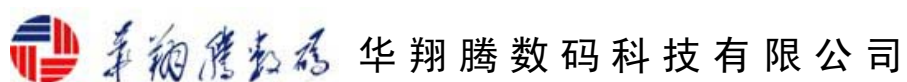


# 华安电子印章系统技术白皮书

---



地址：长沙麓谷高新区麓龙路 199 号标志麓谷坐标 15 楼

邮编：410205

电话：(86) 731-88239608

传真：(86) 731-88239600

网址：[WWW.WallGreat.com](http://WWW.WallGreat.com)

# 目 录

一、技术概述.....	1
二、遵循标准和规范.....	4
三、主要技术特点.....	5
四、系统安全性设计.....	7
五、系统构成.....	10
1、系统组成框图.....	10
2、主要功能.....	11
六、运行环境.....	14
1、服务端运行环境.....	14
2、客户端运行环境.....	14
八、联系方式.....	15

## 一、技术概述

- **公钥基础设施 (Public Key Infrastructure (PKI))**

能够对公钥进行管理并提供身份验证、加解密、完整性以及不可否认性服务的基础设施。PKI 有以下五个基本组成部分：证书认证机构 (CA)、证书库、密钥备份及恢复系统、证书作废处理系统以及应用接口系统。

- **数字证书 (Digital Certificate)**

又称为数字标识 (Digital ID)，它提供了一种在 Internet 上身份验证的方式，是用来标志和证明网络通信双方身份的数字信息文件。基于 PKI 的数字证书中包括的主要内容有：证书拥有者的个人信息、证书拥有者的公钥、公钥的有效期、颁发数字证书的 CA、CA 的数字签名等。

- **电子印章 (Electronic Mark)**

是指以电子形式存在的，依附在电子文件，并与其逻辑关联。可用来辨识电子文件签署者的身份，同时能够保证签署的文件内容完整性，并表示签署者同意电子文件所述事实的内容。

- **数字水印 (Digital Watermarking)**

是永久镶嵌在其它数据 (宿主数据) 中，具有可鉴别性的数字信号或模式，且不影响宿主数据的可用性。通常应用的是图像水印。

- **LSB 变换 (Least Significant Bits Transform)**

即最低有效位变换，是第一个数字水印算法，使用特定的密钥通过 m 序列发生器产生随机信号，然后按一定的规则排列成 2 维水印信号，并逐一插入到原始图像相应像素值的最低几位。由于水印信号隐藏在最低位，相当于叠加了一个能量微弱的信号，因而在视觉上很难察觉。LSB 水印的检测是通过待测图像与水印图像的相关运算和统计决策实现的。作为一种大数据量的信息隐藏方法，LSB 在隐蔽通信中仍占据着相当重要的地位。

- **分块 DCT 变换 (Blocked DCT Transform)**

即分块数字余弦变换，是图像数字水印技术的一类重要算法，通常将图像分割成  $8 \times 8$  的像素块后分别进行 DCT 变换，然后在 DCT 系数的中低频系数叠加水印信息，然后进行反变换后得到嵌入不可见水印的图像。具有抗 JPEG2000 压缩的性能。

- **数据压缩 (Data Compression)**

是通过数学运算将原来较大的文件变为较小文件的数字处理技术，而数据解压缩 (Data Uncompress) 则是把压缩数据还原成原始数据或与原始数据相近的数据的技术。数据压缩通常可分为无损压缩和有损压缩两种类型。无损压缩是指压缩后的数据经过重构还原后与原始数据完全相同，有损压缩是指压缩后的数据经过重构还原后与原始数据有所不同。

- **对称密钥密码体制 (Symmetric Key Cryptosystem)**

也称私钥密码体制，即信息的发送方和接收方用一个密钥去加密和解密数据的密码体制。它的最大优势是加/解密速度快，适合于对大数据量进行加密。

- **非对称密钥密码体制 (Asymmetric Key Cryptosystem)**

也称公钥密码体制，是指信息加密和解密使用两个不同密钥的密码体制。它使用的两个密钥，一个公开发布，即公开密钥 (publickey)，另一个由用户自己秘密保存，即私用密钥 (privatekey)。信息发送者用公开密钥去加密，而信息接收者则用私用密钥去解密。公钥机制灵活，具有较好的安全性。

- **数字签名 (Digital Signature)**

是一种建立在公钥密码体制基础上的用来保证信息完整性的安全技术。其主要方式是信息发送者从报文文本中提取出特征数据 (或称数字指纹，通常是通过 Hash 运算得到的散列值)。发送方用自己的私钥对这个散列值进行非对称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散列值，接着再用发送方的公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。发信者的私钥只有他本人才有，所以他一旦完成了签名便保证了发信人无法抵赖曾发过该信息 (即不可抵赖性)，同时由于签名包含了数据信息，因此保证了数据的不可篡改。

- **VBA (Visual Basic for Application)**

微软的产品 Office 环境下的解释 Basic 语言和内部对象模型，以宏 (Macro) 的形式可以实现用户对 Office 系统的可编程设计和功能扩展。

- **DLL (Dynamic Link Library)**

动态链接库，是用于动态链接的函数库，是 Windows 中的基础程序单元。它使得当

前正在运行的几个程序能够共享一组函数的一个拷贝。

- **API (Application Programming Interface)**

应用程序编程接口，是一套用来控制 Windows 的各个部件（包括从窗口的外观到为一个新进程分配的内存）的外观和行为的一套预先定义的 Windows 函数。

- **COM (Component Object Model)**

组件对象模型，是微软提出的一种实现跨语言、跨系统的通用对象软件中间件模型，可以有效地用于实现应用系统的集成设计和软件的可重用性、可移植性。

- **Office Word COMAddin 接口**

是微软提出的针对 Office 办公系列软件（包括 Word、Excel、Access、PowerPoint）的通用 COM 插件接口标准，可以实现其他应用程序与 Office 系统的无缝集成。该标准定义了 IDTExtensibility2 接口，用于通知应用程序有关 Office 系统的运行和内部对象模型。

## 二、遵循标准和规范

- GB 17859—1999 《计算机信息系统安全保护等级划分准则》
- GB/T 16264.8—200X 《信息技术 开放系统互连 目录 公钥和属性证书框架》
- GB/T XXXXX—200X 《信息安全技术 公钥基础设施 证书格式》
- GB/T 9387.2—1995 《信息处理系统 开放系统互连基本参考模型》
- GB 15851—1995 《信息技术—安全技术—带消息恢复的数字签名方案》
- GB 15853.X—XXXX 《信息技术—安全技术—实体鉴别机制》
- GB/T 17902.1—1999 《信息技术 安全技术 带附录的数字签名》
- GB/T 17903.X—1999 《信息技术 安全技术 抗抵赖》
- GB/T 17143.8—1997 《信息技术 开放互连系统 系统管理 安全审计跟踪功能》
- 《证书认证系统密码及其相关安全技术规范（试行）》 2004.6
- 《国务院关于国家行政机关和企业、事业单位印章的规定》
- 《民办非企业单位印章管理规定》
- 《印铸刻字业暂行管理规则》
- 《社会团体印章管理规定》
- 《民政部、公安部关于印发〈社会团体印章管理的暂行规定〉的通知》
- 《社会力量办学印章管理暂行规定》
- 《中华人民共和国电子签章条例》
- 《中华人民共和国电子签名法》
- 《中国共产党机关公文处理条例》
- 《国家行政机关公文处理办法》
- 《国家行政机关公文格式》
- 《国务院办公厅关于实施〈国家行政机关公文处理办法〉涉及的几个具体问题的处理意见》
- 《湖南省行政机关公文处理办法》

### 三、系统技术特点

华翔腾公司自主研发的 SJY105 电子印章系统是通过国家密码主管部门的技术鉴定和公安部计算机信息系统安全专用产品检测的商用密码产品，它基于 PKI 技术体系，利用现有的网络资源，为用户提供电子印章的制作、管理、撤销、签章、验章等功能，满足了电子印章在制作、使用、验章、撤销等业务上的安全性需求，同时可保证了签章文件和电子印章的完整性、权威性、合法性、唯一性与不可抵赖性。该产品依据《中华人民共和国电子签名法》，严格遵循国家密码安全的相关标准和规范进行设计，支持国家密码主管部门批准的密码算法，它具有以下特点：

#### ➤ 完全基于 PKI 标准

PKI 即“公开密钥体系”，是一种遵循既定标准的密钥管理平台，它是为所有网络应用提供加密和数字签名等密码服务的一种密钥和证书管理体系。简单来说，PKI 就是利用公钥理论和技术建立的提供安全服务的基础设施。PKI 技术是信息安全技术的核心，也是电子商务、电子政务的关键和基础技术。

#### ➤ 符合国家商用密码规范

系统核心模块—华安电子证书认证系统采用通过国家密码管理局安审和鉴定的 PCI 密码卡和 USB 智能卡钥匙，并采用国家密码管理局批准的密码算法实现对称加解密处理。所有非对称的签名和解密处理以及对称的加解密处理都是由硬件完成的。

系统通过了国家密码主管部门组织的安全性审查，国密局批准的商用密码产品型号为 SJY105 电子印章系统。

#### ➤ 安全性高

- ✓ 只有一定权限的用户才能进行相应操作，数据库中的数据应要求获得安全性保障；
- ✓ 用通过国家密码管理局安全性审查和鉴定的数据密码卡产生 RSA 算的公钥和密钥，自主开发的华安电子证书认证系统生成 ITU-TX509 国际标准定义的数字证书；
- ✓ 用数字证书和位图图章绑定，确保电子印章来源可靠；
- ✓ 在电子印章中绑定数字水印，防止非法拷贝印章位图；

- ✓ 采用标准的散列算法 (HASH) 产生数字摘要，确保电子签章和被签文件紧密绑定；
- ✓ 采用国家密码管理局批准的对称密码算法加密电子签章实体数据；
- ✓ 采用国家密码管理局安全性审查和鉴定的 SecurityKey 存储密钥，与软件联合控制签章权限；
- ✓ 通过签章记录可追溯从制章签章到当前签章的全过程；
- ✓ 文件的传输采用自主开发的安全电子邮件。

### ➤ 功能强大

- ✓ 可在文件上添加电子签章，就像我们常用的纸质公文上的签章效果；
- ✓ 可在线 (Internet) 或离线签章；
- ✓ 可将电子签章和文件紧密绑定 (整个文件或文件部分)，一旦绑定区域被篡改，电子签章将失效；
- ✓ 可随时对电子签章的可靠性及其绑定的部分的完整性进行验证；
- ✓ 可控制文件打印权限及打印份数，以及可随时锁定文件；
- ✓ 动态配置文件流转方式和流转过程，并且可以进行人工干预。

### ➤ 技术先进

- ✓ 采用 COM 组件的技术，将电子签章和文件紧密绑定；
- ✓ 模块化设计原则，确保系统的扩展性：电子印章制作，电子印章签章验章，公文流转（公文拟稿、会签、清稿，安全电子邮件）；
- ✓ 透彻地研究了相关应用平台的 SDK，确保代码兼容性和运行稳定性；
- ✓ 采用国家密码管理局批准的算法进行加解密和数字签名处理，在数据传输时，利用上列算法进行数据加密封装；
- ✓ 对文件的操作权限与功能按钮配套出现。

### ➤ 标准化程度高

- ✓ 依据国家有关印章管理的规定生成位图图章；
- ✓ 根据国家行政机关公文格式生成红头文件模版；
- ✓ 采用国际标准 X509 生成电子证书；

### ➤ 使用方便

- ✓ 采用浮动菜单的样式放置功能按钮，轻轻一点就可对文件作相关操作；
- ✓ 采用自行设计的华安安全电子邮件方式传输文件。即使在异地，也可通过互联网对文件进行会签、签章；
- ✓ 具有联机帮助和疑难解答等帮助系统。

## 四、系统安全性设计

### ◆ 物理防护措施安全

依托于华安电子证书认证系统，作为一个企业级的应用系统，必须将密钥管理中心、证书管理中心和核心数据库（密钥数据库、证书数据库、印章数据库和文档数据库）放置在具有门禁系统的独立环境中。通过管理制度授权相关人员才能进入，进行系统的设置和维护。所有密钥均保存在专用加密设备中，从物理上保证了系统的安全。

### ◆ 密钥管理安全

华安电子证书认证系统密钥管理中心所使用的密钥是由通过国家密码管理局安全性审查和鉴定的专用硬件高速密码卡生成。根密钥存放在 PCI 密码卡中，根密钥对的公钥经系统签名的生成自签名证书。

所使用的密钥包括签名证书和加密证书的两对非对称密码算法的公、私钥对以及国家密码管理局指定的对称算法的密钥两种类型。

用户申请加密证书和签名证书，证书管理中心签发证书后，将证书和密钥文件一同通过安全信道发送给证书注册管理系统，证书注册管理系统自动将证书和密钥导入的 SecurityKey 中，用户修改 PIN 码后颁发给用户。其中加密证书的私钥在数据库中有备份，而签名证书的私钥由用户的密码钥匙产生并存放。

### ◆ 加解密算法安全

数据加解密算法采用国家密码管理局批准的非对称密码算法和对称密码算法，加密操作和签名操作都在通过国密办鉴定的专用硬件设备中完成，系统将数据准备好后，将其送到密码卡内进行处理，处理完毕，再将结果返回。整个加解密和签名的过程中，关键信息不会泄漏到内存中。

### ◆ 身份认证安全

通过系统的证书系统实现身份认证，应用 PKI 机制实现对使用者身份的认证，高强度的

密码加密技术保障了身份认证的安全性。

### ◆ 制章人身份认证

系统制作的电子印章嵌入了印章制作人的签名信息：印章制作人用自己的 SecurityKey 对印章图片进行签名，并把签名证书 ID 号和签名信息作为不可见水印嵌入到了印章图片中。其他人可以根据印章拥有人的签名证书 ID 号从 LDAP 中下载其签名证书对印章进行认证，也可以利用证书认证系统提供的客户端插件对印章制作人的身份进行在线认证。

### ◆ 印章拥有人身份认证

系统制作的电子印章嵌入了印章拥有人的签名信息：印章拥有人用自己的 SecurityKey 对印章图片进行签名，把签名信息作为不可见水印嵌入到了印章图片中。在印章中同时嵌入了拥有人的签名证书 ID 号。其他人可以根据印章制作人的签名证书 ID 号从 LDAP 中下载其签名证书对印章拥有者的身份进行认证，也可以利用证书认证系统提供的客户端插件对印章拥有者的身份进行在线认证。

### ◆ 签章人身份认证

签章人在签章前从数据库中提取印章，首先比较 SecurityKey 中签名证书的 ID 号与印章在用库中相应印章所嵌入的拥有人的签名证书 ID 号是否一致，只有在两个证书的 ID 号相同时才表明签章人可使用此章。也就是说保证只有印章拥有人才能使用自己拥有的印章。

签章时，在印章中嵌入了文档的签名信息。

手写批注的图片中嵌入了审阅者对所绑定部分的文本信息的签名，同时嵌入了审阅人签名证书的 ID 号。

经过上面的处理（签名+数字水印），电子签章用户在文件上的签章和具有手写批注权限的审阅人在文件上所作的手写签名，就可以由其他合法的阅读用户以及进行其他操作的合法用户进行身份认证，以确保签章和签名的正确性以及文档的完整性，从而确定对文档是否接受和承认，以及确定是否进行下一步的操作。

### ◆ 操作权限的身份认证

在流转中心配置好操作权限以后，文档和权限被封装为加密的二进制流文件 (\*.dsm) 后利用邮件发送给相应的操作人。文档主体是经过压缩后，再用对称算法进行加密，其密钥是由 SecurityKey 自身随机产生的，该密钥用接收方的加密公钥进行加密。接收方必须用自己的 SecurityKey 中的加密私钥才能打开文档，获得相应权限，进行相应操作。也就是说没

有相关操作权限的人就无法打开文档或进行其他操作。

## ◆ 相互间通信安全

在文件流转过程中，采用自主开发的安全电子邮件。

(1) 发送方用接收方的加密公钥加密对称加密算法的密钥，连同加密文档一起发送给接收方，接收方用 SecurityKey 解密数字封装的算法密钥，再用其解密 .dsm 文档，同时知道了自己相应的权限。

(2) 自主开发的邮件发送、接收功能以及后台监控程序，可以自动下载 dsm 类型文件，同时把邮箱中的对应邮件删除。

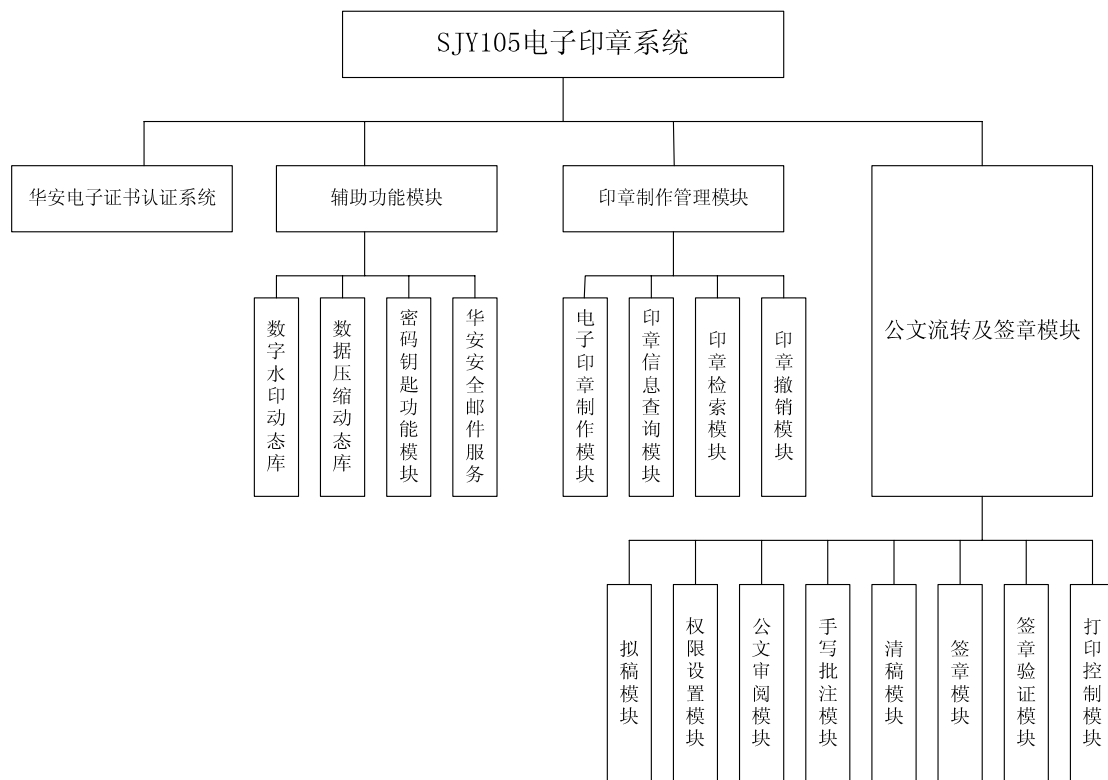
(3) 对 word 文件按照权限操作完毕后自动完成 (1) 中所描述的工作后发送，再自动删除当前目录下的上述文件。

## ◆ MS Office 系统的安全性实现

印章系统的插件直接嵌入微软公司的 Office 系统，对 Office 在文档保护方面采用了一些安全增强措施。它的安全性保护主要体现在文档的阅读控制和文档的锁定。文档的阅读控制是利用设定打开密码，只有打开密码正确才能打开文档。文档的锁定有批注锁定、修订锁定和只读锁定。这些功能都只在一定的条件下起作用。利用 Office 的这些功能，同时基于 PKI 技术强化了这些功能，其主要目的是权限和身份认证，做到了无缝连接。

## 五、系统构成

### 1、系统组成框图



## 2、主要功能

### ■ 华安电子证书认证系统

华安电子证书认证系统（以下简称“认证系统”），是华翔腾数码科技有限公司面向政府、行业部门、企业等开发的，适用于组织机构内部的数字证书与密钥管理系统。它可为身份认证以及其它安全应用系统的配套安全性基础设施服务，也可以扩展为上级认证系统的子系统，完成多级认证系统的配置。

华安电子证书认证系统提供了对生存周期内的数字证书进行全过程管理的功能，包括用户注册管理、证书/证书注销列表的生成与签发、证书/证书注销列表的存储与发布、证书状态的查询、密钥的生成与管理以及安全管理等。

具体介绍请参见华翔腾公司的《华安电子证书认证系统技术白皮书》。

### ■ 公文流转

#### 1) 人事信息管理功能

对签章系统中的角色进行定义。

#### 2) 拟稿功能

实现新建文档、打开已有文档或模版等功能。

#### 3) 审阅、清稿权限设置功能

根据具体人事信息和文档属性设定人员对文档的审阅、清稿权限。

#### 4) 审阅功能

保留对文档的修改痕迹，不同的人有不同的颜色和删除线，也可在修订处加入修改内容，不能删除他人的修改内容，高亮显示修改人和日期，可见他人的修订内容。

#### 5) 手写批注功能

提供手写批注和签名功能。

#### 6) 清稿功能

根据需要，可自动（或手动）接受（或拒绝）审阅修改内容，对文档定稿。

#### 7) 签章打印权限设置功能

根据人事信息和文档属性设定人员是否具有打印文稿的权限。

## 8) 签章功能

选择所需印章，在用户指定的位置盖一个或多个印章（可进行位置微调），印章上浮显示，不遮盖文字。

## 9) 签章验证功能

可验证文档的完整性和印章的正确性。

## 10) 删除签章功能

可由原签章人在文档未正式发布前删除自身所作的签章信息。

## 11) 文档作废功能

文档内容失效或者发生关键性错误，由原签章人对所签印章做作废处理，以示文档内容无效

## 12) 打印控制功能

无权限的用户无法打印，并控制打印文档份数，使之不超过设定的份数上限。

## 13) 邮件服务功能

文档通过华安安全电子邮件实现公文网上流转。可实时监控。保证安全和效率。

## 14) 帮助功能

为用户使用本系统提供帮助。

## ■ 印章的制作和管理

### 1) 原始位图制作功能

经有关部门审批后，可根据制章人输入的信息快速制成专业的可见印章原始位图（未嵌入任何信息）。

### 2) 半可见图形嵌入功能

将用户指定的位图以半可见水印方式嵌入印章原始位图之中，生成新的印章位图。

### 3) 签名信息嵌入功能

将制章人和印章拥有人的证书信息（如用户名、证书序列号、印章制作时间等）以及他们对 B 中位图的签名信息以不可见水印的方式嵌入印章位图之中，生成最终的电子印章。

### 4) 数据库存储功能

将电子印章（位图以及相关信息）存储至数据库中，防止印章被非法篡改。

#### 5) 印章信息查询功能

合法用户能查询其名下任何一个印章的全部信息。

#### 6) 印章检索功能

合法用户可任意选择字段（如用户名、证书序列号、印章制作时间等），进行匹配查询，检索得到符合条件的全部印章。

#### 7) 印章撤销功能

制章人在需要时，可将已制作或发放的印章作废（由在用数据库转至历史数据库中），并在日志数据库中记录，同时录入撤销印章的批文信息。

#### 8) 电子印章日志功能

管理、跟踪和监控电子印章的制作和使用情况。

### ■ 辅助功能

#### 1) 水印嵌入和提取功能

将不可见、半可见水印嵌入印章位图之中，并可将相应信息提取出来。

#### 2) 数据压缩/解压缩功能

对文档进行无损压缩/解压缩操作，以便通过安全电子邮件进行传输。

#### 3) 对称加解密功能

对文档（按二进制数据方式）进行对称加解密。

#### 4) 非对称加解密签名功能

对文档实施签名/验证、对数据流加解密。

## 六、运行环境

### 1、服务端运行环境

#### ➤ 证书认证系统

- ✓ 数据库服务器一台。
- ✓ 密钥管理服务器一台。
- ✓ 证书管理服务器一台。
- ✓ 证书注册管理服务器一台。
- ✓ Web 服务器一台。
- ✓ LDAP 服务器一台。
- ✓ OCSP 服务器一台。

#### ➤ 公文流转和电子签章管理系统

- ✓ 数据库服务器一台；
- ✓ 制章服务器一台；
- ✓ 流转中心服务器一台

所有涉及的设备均按功能或业务划分，可在同一设备上实现多种服务端的功能，具体部署数量以系统的规模大小确定。

### 2、客户端运行环境

- ✓ 中文 Windows2000/XP 操作系统；
- ✓ 显示模式：真彩色 32 位；
- ✓ MS Office, 推荐 MS Office 2003；

## 七、典型案例

- ✓ 岳阳市县乡机要部门安全公文传输系统：安全电子邮件+SJY105 电子印章系统。
- ✓ 江西省县乡机要部门安全公文传输系统：安全电子邮件+SJY105 电子印章系统，典型用户包括南昌、吉安、新余、上饶、萍乡、抚州。

## 八、联系方式

如需获得更新或者更多资讯敬请通过下列方式与本公司联络。

### 华翔腾数码科技有限公司

中国 • 湖南

地址：长沙麓谷高新区麓龙路 199 号标志麓谷坐标 15 楼

邮编：410205

电话：(86) 731-88239608

传真：(86) 731-88239600

网址：[www.WallGreat.com](http://www.WallGreat.com)

本资料为华翔腾数码科技有限公司版权所有，严禁非法复制。