

为何西讯® ERP 公文管理系统无需“电子印章”？

北京环宏软件技术有限公司

企业管理咨询部

2007 年

西讯® ERP 管理系统公文管理系统是根据中国行政机关和大型企业管理的需要而开发的公文辅助管理系统，其目的是为原来完全依靠纸张传递的公文系统提供一个电子的副本，便于快速传递和查询。

西讯® ERP 管理系统公文管理系统的功能包括：

- 1、根据用户自己设定的流程，在电脑上完成拟文、审核、发布、归档等工作；
- 2、每个用户可以根据自己的权限看到与自己相关的文件，不会遗漏；
- 3、用户可查询已经归档的历史文件，检索相关内容；
- 4、某些文件可以和相关的业务管理系统集成使用。例如人事任命文件可以和人力资源管理中的职务变动记录关联，用户可以从人事档案查到原始的人事任命文件。

公文作为政府行政机关和大型企业传统上用于管理的主要手段和命令系统，必须满足可靠保密性、不可更改性和有效性等三个基本安全原则。那么，传统的纸张文件加公章是如何满足这种安全原则的呢：

可靠性：加盖公章的文件可以从纸张和公章来判别真伪，一般情况下无法伪造。在传送的过程中通过盖章加封可以保证其机密性，只有授权人员才能看到；

不可更改性：纸张文件的更改会留下比较明显的痕迹，一般情况下不易更改；

有效性：如果确认文件和公章是真实的并且未经篡改，一般就认为有效，可以执行；

当我们将纸质公文复制为电子公文（以电子数据方式存放在电脑系统中）时，并且要异地传输和执行时，也必须满足安全性和有效性这两个条件。不同形式的电子公文将会以不同的方式来保证这两个条件。

电子公文可以分为两大类：

- (1) 以某种独立文件格式存在的公文。例如以微软 Word 文字处理文件格式保存的文件，以普通 text 文本格式保存的文件，或者以 Adobe 公司的 pdf 格式保存的文件等。这类文件本身不提供任何有价值的安全性，任何人都可以进行修改和编辑。所以，未加任何其他安全措施独立文件格式不能直接用于公文的处理和传输。
- (2) 以大型安全数据库形式保存的公文，例如微软的 SQL 数据库或者甲骨文的数据库等。由于数据库本身带有极高级别的安全系统，不仅可以保证数据存储的安全，也可以通过客户端-服务器端的加密通道，保证数据传输过程的安全。所以存放在数据库中公文远比文本型数据安全，同时其传输过程也更为安全。

西讯® ERP 管理系统公文管理系统是一种基于微软的 SQL 数据库的公文管理系统。公文数据是以数据库的方式存放在电脑中，用户必须跨越西讯® ERP 系统的应用级安全屏障和 SQL 数据库的系统级安全屏障才能访问或者修改数据。与文件型数据不同（原则上，文件型数据只要传到你的电脑上，你就可以对此进行修改），西讯® ERP 的公文数据是存放在服务器数据库中，未获得授权的人是不可能对此进行任何改动，从而保证了公文数据的来源的可靠性和文件的不可更改性，最终保证其有效性。所以，不需要采用任何额外的公私密钥加密方法（也就是无需采用任何所谓电子印章），西讯® ERP 的公文管理即可保证其安全性。

如何使用公私密钥安全传送文本型电子数据？

文本型的电子文件一旦离开创建者电脑，便没有安全性可言。无任是通过软盘、U 盘等电子媒体，或者通过 Internet 网络传送，都无法保证该文件在传送的过程中没有被篡改，收件者也无法确认该文件的真伪。所谓安全的传送，就是要保证两点：

- 1、收件人可以肯定该文件来自已知的发件人，而不是其他人伪造的；
- 2、收件人可以肯定该文件未被改动；

为此，我们必须使用公私密钥来对文件进行加密。公私密钥加密方式是目前最先进的加密方式之一。它的原理如下：

公钥：可以公开的一组数字标识

私钥：自己秘密保留的一组数字标识

使用配对的公钥和私钥都可以对文件加密，但是用公钥加密的文件只能用配对的私钥解密，反之用私钥加密的文件只能用配对的公钥解密。

假设甲乙两人各有一组公私密钥。每个人都拥有自己的私钥和对方的公钥。如果甲要传送一个文件给乙，希望该文件只能让乙看到，并且不能被篡改。于是，甲用自己的私钥加密，然后再用乙的公钥加密。当乙收到文件后，先用自己的私钥解密（如果成功，表示除了加密者之外没有任何人见过该文件），再用甲的公钥解密（如果成功，表示该文件确实来自甲），即可得到完整的文件。

什么是“电子印章”？什么是数字签名？什么是数字标识？

电子印章并非电子文件中可看到的印章图像。任何电子文件中的图像都是极易篡改的。所谓电子印章实际上就是以公私密钥加密的文件。市场上有许多加密软件或者应用软件都支持公私密钥加密。其中最典型的可以说是我们每天都在用的微软公司电子邮件程序 Outlook Express。通过使用 Outlook Express 的“数字标识”，您可以在电子事务中证明您的身份，就像兑付支票时要出示有效证件一样。您也可以使用数字标识来加密邮件以保护个人隐私。

数字标识由公用密钥、私人密钥和数字签名三部分组成。当在邮件中添加数字签名时，您就把数字签名和公用密钥加入到邮件中。数字签名和公用密钥统称为证书。您可以使用 Outlook Express 来指定他人向您发送加密邮件时所需使用的证书（就是你的公钥）。

收件人可以使用您的数字签名来验证您的身份，并可使用公用密钥给您发送加密邮件，这些邮件必须用您的私人密钥才能阅读。要发送加密邮件，您的通讯簿必须包含收件人的数字标识。这样，您就可以使用他们的公用密钥来加密邮件了。当收件人收到加密邮件后，用他们的私人密钥来对邮件进行解密才能阅读。

总的来说，使用数据库的专业管理系统是比一般文件系统更为高级和安全的处理系统，使用也更加方便可靠，完全没有必要再使用任何“电子印章”。

“电子印章”一般只用于传输独立的文本型的数据文件。

文本型电子文件如何实现不可更改性？

一个已经批准执行的公文，我们不希望其在传送、拷贝、打印等处理过程中被篡改，哪怕无意的更改。为此，Adobe 公司发明了 PDF 文件格式（Portable Document Format 可携带文件格式），PDF 文件一经产生，便不可再改动（包括其版面、图形、文字等）。阅读 PDF 文件需要 Adobe 公司提供的免费阅读软件。当然产生 PDF 文件的软件就不是免费的。PDF 文件已经成为事实上的不可更改文件格式的国际标准。当然，也有许多别的公司发明了各种不同的不可更改文件的格式，分别用于各种特别的领域。特别需要指出的是，电子文件的不可更改性是相对的，而可更改性则是绝对的。使用特殊的软件也可以更改 PDF 文件。

相比之下、数据库的不可更改性要比文本文件强大许多倍。

当然，西讯® ERP 管理系统公文管理系统并不能完全替代纸质公文。已经批准执行的公文仍然应该打印盖章存档，以备应急查询。

西讯® ERP 管理系统公文管理系统完全满足公文处理系统要求的可靠保密性、不可更改性和有效性等三个基本安全原则。在实际的工作中可以起到纸质公文同样的效果，而且效率更高，更为方便。

北京环宏软件技术有限公司

北京市海淀区长春桥路 5 号新起点嘉园 2 号楼 2208 号

邮编 100089

电话： (10) 82563073

传真： (10) 82562183

电子邮件： sales@westinfo.net

网站： www.westinfo.net