安全电子公文交换系统解决方案

(By WoSign, 2007.05)

一、存在问题

公文的上传下达是我国各级政府和大型企事业单位中长期依赖的一种工作手段和重要工作内容，传统的公文交换方式主要采用邮递和直接送达方式传递红头文件，但具有速度慢、易泄密、易丢失、成本高等不足，所以，现在已经有许多政府机关和大型企事业单位采用了各种各样的电子公文交换系统，实现公文传递的电子化和即时化，从而大大提高办公效率。

但目前的电子公文交换系统普遍的不足就是信息安全问题，主要表现在：

(1) **真实身份认证问题**：涉及到两个真实身份的认证问题，一个是访问公文交换系统的用户的真实身份认证，另一个是交换系统本身的真实身份认证。而前者最重要，因为仅凭简单的“用户名＋口令”的传统身份认证方式根本就没有任何安全性可言，从而失去了公文交换系统的保密性要求。

(2) **公文的机密性和完整性问题**：公文交换系统用户在访问公文交换系统时要求用户输入用户名和密码以及其他机密信息和通过身份认证后从服务器传来的机密信息，从用户端电脑与服务器之间的机密数据的传输过程中要经过许多网络设备和传输链路，如果此类机密信息不加密传输，则非常容易和极有可能在传输过程中被非法截取而泄密，这是非常危险的，将有可能泄露企业商业秘密，甚至国家机密。同时，如果在用户端电脑到交换系统数据库服务器之间的所有信息交换在传输过程中不加密的话，则非常容易和极有可能在传输过程中被非法恶意篡改，将会给国家和企业蒙受巨大的损失，而用户本身还不知晓。

(3) **不可否认性问题**： 不管是公文的签发单位还是接收单位，所有用户有可能会否认其在线操作行为，这里有许多原因，可能是用户本身的原因，也可能是其他方面的原因，而每个在线操作一定要有可靠的签名记录用于纠纷仲裁的法律依据。

(4) **无纸化和有纸化冲突问题**： 许多政府系统和企业的公文交换系统失败的原因在于并没有真正无纸化，既要用电脑，又要用纸，不仅增加工作量，而且好像是否有此系统都一样而使用用户不愿意使用无纸化办公系统。问题在于并没有彻底解决好无纸化和有纸化的冲突问题，要上系统就要彻底无纸化，丢掉纸和笔。此问题看起来好像与信息安全无关，但实际上是数字签名(数字盖章)的问题，当然有关。

二、解决方案

针对以上安全隐患和可能出现的问题， WoSign 推出了基于 PKI 技术的安全公文交换系统信息安全解决方案，完全解决了以上 4 大问题：

(1) 为公文交换服务器(Web 服务器、邮件服务器和其他应用服务器)部署全球通用的支持所有浏览器的强制 128 位加密的 SSL 证书，确保用户在任何地方都可以安全地访问文件交换服务器，支持从浏览器到服务器之间机密信息的高强度加密传输，从而有效地防止了机密文件信息在文件传递过程中的非法窃取和非法篡改，保证了公文的机密性和完整性。

(2) 为每个文件交换系统的用户颁发一个全球通用的个人数字证书或单位数字证书用于登录文件交换系统的真实身份认证和用于每个在线操作的数字签名，从而杜绝了口令泄露而造成的损失和提供了交易不可否认的证据。为了杜绝使用公用电脑和专用电脑的间谍软件或其他可能的手段非法使用数字证书问题，强烈推荐用户使用 USB Key + 数字证书方式来确保是真实的合法用户安全地登录文件交换系统(需要登录和在线处理业务时就把 USB Key 插入电脑的 USB 口，用完就拔下) 。如果是使用电子邮件系统来实现文件交换，则此证书将用于交换文件的电子邮件的数字签名和加密，实现全程的安全的电子邮件方式文件交换。不仅如此，为了防止用户非法访问 Web 服务器上的内容，可以在 Web 服务器上设置此允许某些或某种特征的客户端证书才能访问服务器，直接从服务器端物理控制访问权限。

(3) 无论是 Web 方式和电子邮件方式实现文件交换，所有公文的签发都必须使用 Adobe Acrobat 来制作成 PDF 格式文件，并使用公文签发单位的数字证书数字签名公文文件，充分利用 Adobe Acrobat 提供的签名文档和验证文档功能在线签署公文，从而彻底丢掉纸、笔和公章，解决无纸化和有纸化的冲突问题。为了确保文件签名的权威性，PDF 签名证书仅使用 USB Key 为证书载体，需要签名和签署文件时把 USB Key 插入电脑中即可。而如何需要收文单位签署意见或证明已经正常收文，也可以要求收文单位在文件上数字签名和签署意见。

以上解决方案涉及到的产品有：服务器 SSL 证书、客户端数字证书和 PDF 文件签名证书，请浏览以下页面了解产品详情，我们不仅提供相关产品，而且免费提供开发和应用指导：

服务器 SSL 证书： http://www.wosign.com/products/sgczhenssl.htm

PDF 文件签名证书： http://www.wosign.com/products/docsigning.htm

客户端数字证书： http://www.wosign.com/products/clientcert.htm

使用数字证书实现强身份认证登录演示：https://www.wosign.com/logindemo/

服务器安全访问控制解决方案：http://www.wosign.com/solution/Access_Control.htm

如果您就是政府有关部门和大型企业的信息主管，请重视公文交换系统的信息安全建设，并请联系我们，我们有更详细的方案发给您；如果您是企业的员工或政府公文交换系统的用户，请把我们的解决方案报告有关部门的信息主管以便尽快采取有效的信息安全防范措施，只有大家齐努力才能确保公文交换系统的信息安全，WoSign 愿意为此做出应有的贡献。

注：此 PDF 文件已经数字签名，并已模拟有几个人签名已阅，供参考。

WoSign Support Team

数字签名人 WoSign Support Team
DN：cn=WoSign Support Team,o=WoSign, Inc., ou=WoSign Employee, email=support@wosign.com
原因：我是该文档的作者
日期：2007.10.18 13:49:03 +08'00'

WoSign Customer Service Team

数字签名人 WoSign Customer Service Team
DN：cn=WoSign Customer Service Team,o=WoSign, Inc., ou=WoSign Employee, email=cs@wosign.com
原因：我证明本文档是准确和真实的
日期：2007.10.18 13:49:43 +08'00'

深圳市沃通电子商务服务有限公司

电话：0755-3363 3000

传真：0755-3397 5112

网站：www.wosign.com

Email: support@wosign.com

