上海轮胎橡胶（集团）股份有限公司

数字签名帮助无纸化办公

本方案基于Microsoft的平台

Windows 2003 Server
Windows 2003

本方案基于Microsoft的产品：

Microsoft Office
Windows 2003 Server CA

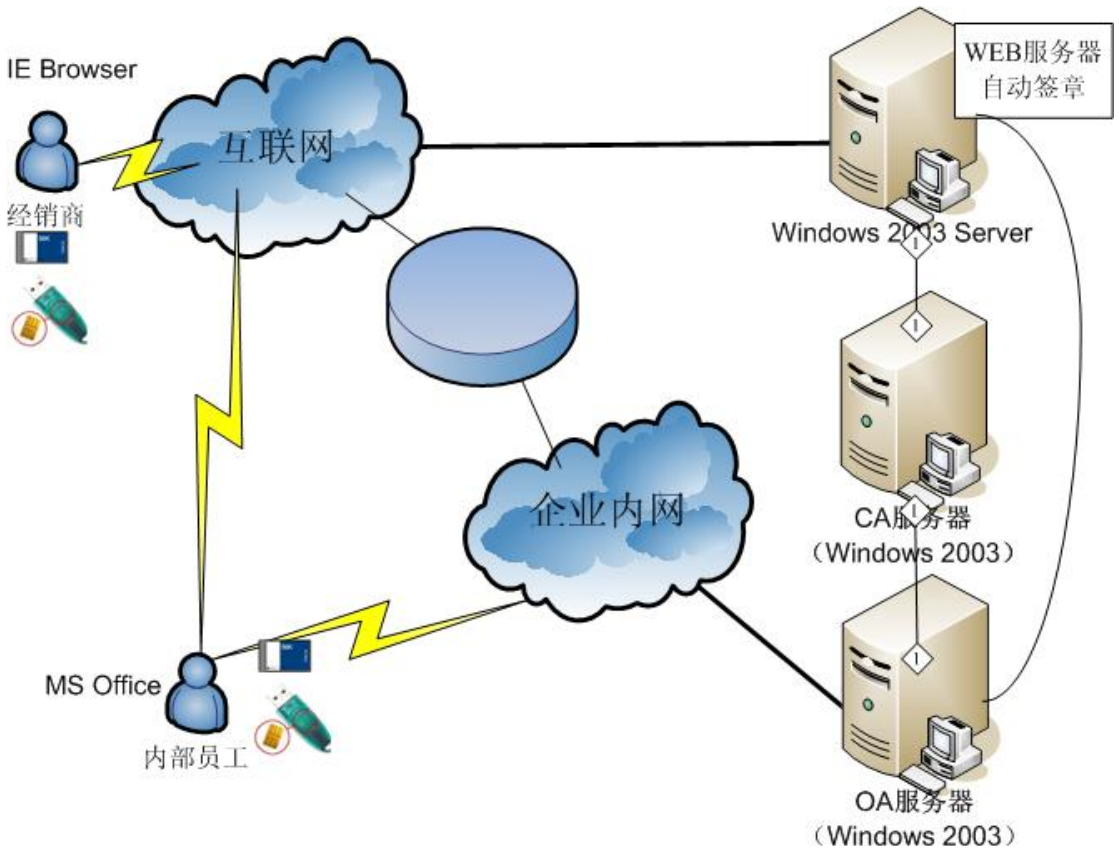
解决方案介绍：

解决方案全称：数字签名帮助无纸化办公
开发商：上海龙方信息技术有限公司

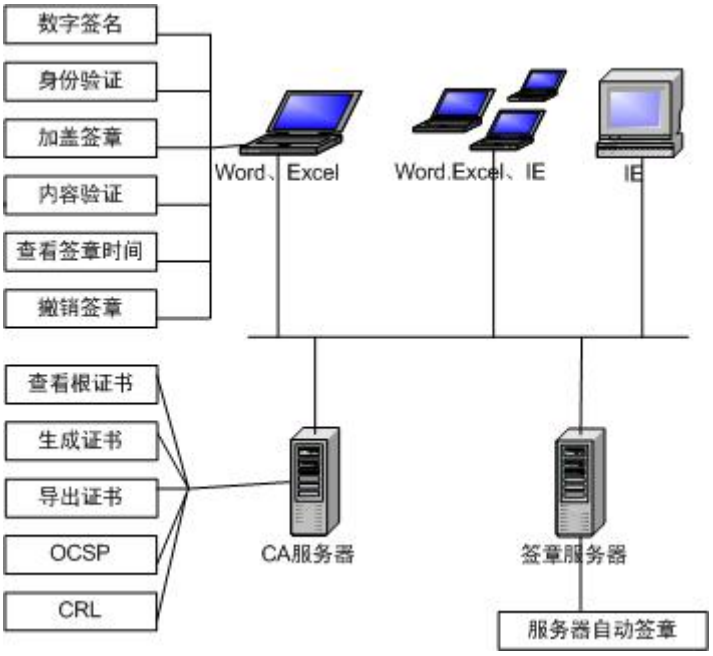
简介

上海轮胎橡胶（集团）股份有限公司是上市的国家一级企业，是国内知名的轮胎制造、轮胎研究、轮胎出口的综合性大型企业，拥有几千名员工。为了提高公司内部整体的行政办公审批流程的效率，进一步实现无纸化网络办公的目标，轮胎橡胶采购了龙方的基于 MS Office 的数字签名软件供内部人员办公之用，同时，他们采用 Windows2003 服务器中的 CA 功能，进行网络化的签名认证和数字证书的管理。轮胎橡胶也采购了龙方基于 Web 的数字签名和在服务器中自动签名的产品，为他们与分销商之间的网上 B2B 电子商务奠定了良好的安全信任的技术基础。

从下面的网络拓扑图中可以看出，龙方的数字签名和微软的终端软件和服务器端软件相配套，无缝使用，为办公自动化和电子商务提供安全、可靠的解决方案，同时也帮助企业创建二十一世纪的无纸化、高效率办公环境。



下图从功能的角度介绍了签名软件和 CA 服务器：



本系统中数字签名系统功能结构图

系统功能介绍：

1.签章过程

USBKey 登陆

系统必须通过 USBKey 登陆。签署者的密钥信息以及证书信息存放在 USBKey 中，USBKey 通过 PIN 码保护，能够确保私钥不出 Key，签名运算在 USBKey 内进行，从而保证了运算过程的安全性。ID-Sign 的签名运算使用了 USBKey，用户的密钥信息和证书信息存放在 USBKey 中，方便用户的携带，及随时随地都可以进行登陆或签名。

身份验证

利用签署者的证书颁发机构的证书，对签署者的身份进行认证。一方面能够辨别签署者身份的真伪，另一方面能够确保签署者身份的不可抵赖性，即一旦签名而且身份认证通过，则签名者将无法否认此签名。

加盖印章

对多个信息域进行数字签名，并可以加盖签名或图章。能够在任意地方显示印章或手写签名。

内容验证

主要是验证内容是否被篡改，如果内容被篡改，则提示“签名无效”，被篡改处会显示红色，印章上会出现横线。

撤销签章

在提交之前，验证没有通过的，用户可以撤销签章，进行修改确认后再盖章。

签章时间

签章时间是签章人签章时的系统时间，为了增加其严密性，系统提供相应接口，可从服务器上获取标准时间戳。

2. 签章验证过程

完成对签章的完整性以及签章人证书的正确性进行一系列的验证。具体能够完成如下功能：

查看证书

任何人都可以查看签署者的数字证书信息，查看证书信息时不需要提供 USBKey。

内容验证

主要是验证内容是否被篡改，如果内容被篡改，则提示“签名无效”，被篡改处会显示红色，印章上会出现横线。

签章时间

签章时间是签章人签章时的系统时间，为了增加其严密性，系统提供相应接口，可从服务器上获取标准时间戳。

OCSP 验证

通过颁发证书机构的 CA 服务器来验证签名信息。

CRL 验证

通过证书撤销列表来验证签名有效性。

系统环境：

软件：Windows 2000/XP/2003; Office 2000/XP/2003， Windows2003 server 企业版

硬件：USBKEY(Safenet, Ftsafe, esafe, etc) 或智能卡（Gemplus）