



## 技术与解决方案

Technologies and Solutions

# 新华人寿保险公司办公系统中 USBKey 的应用

在传统的企业的自有的网络中，企业中的各个分支机构、及其客户是通过专用的线路连接的，既企业的员工之间、企业与其客户之间使用专门的网络设备相互连接在一起。随着Internet的应用、以及电子商务的不断的的发展，企业员工移动办公的现象越来越普遍，企业的业务分支机构及其客户的分布越来越广泛。传统的网络连接的方式越来越无法适应此种商务模式。因此越来越

在此环境下,企业将面临着多种威胁,如企业的员工通过Internet下载和上传企业的敏感的信息,并信息未经过加密,被别人窃听。如入侵者试图不经过授权来访问企业的敏感的信息。如病毒、间谍软件等不健康的软件试图侵入企业内部的主机,并这些侵入是可能通过一个被信任的用户的一些日常的通信行为,如打开一个E-mail的附件或者下载一个文件。

企业需制定网络的使用者及其访问的信息资源的安全方针,既这个用户或者组用户可以对那些信息资源进行读、或者写、或者执行的操作。

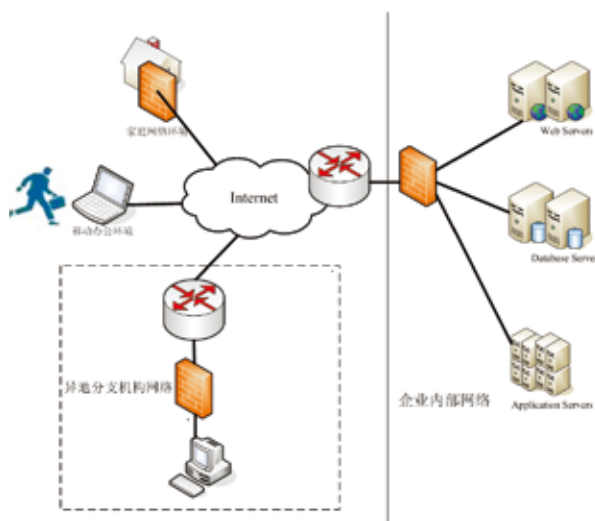
企业需制定网络的使用者所传输的信息的安全方针,既那些信息需要加密、那些信息需要防篡改、那些信息需要防止被否认。

企业需制定主机的安全方针,既在主机上安装那些操作系统、入侵检测系统、反病毒系统、应用系统、数据库系统等。

企业还需制定审计的方针,既定期审计网络的使用者及所访问的资源的审计记录、主机的审计记录、以及应用系统的使用审计记录等。以便审计和跟踪安全事件的发生、运行、及结果。

由此可见,不可否认的强认证系统和对信息的保护是满足以上需求的基本条件,使用智能卡的PKI证书认证系统可以实现用户登录安全认证、传输数据的机密性保护、完整性检查和抗抵赖性。新华人寿保险公司的安全办公系统充分尊重所面临的这些风险,采用PKI技术作为保障公司信息安全的方案,并采用飞天诚信公司的ePass3000 USB Key作为保存和应用RSA密钥对和证书的基础设备。

飞天诚信公司的ePass系列USB Key产品广泛的支持基于PKI的证书应用系统,在各个行业都得到了广泛的使用。在新华人寿保险公司的安全办公系统中,飞天诚信公司的ePass3000支持Windows域登录、支持Juniper SSL VPN客户





## 技术与解决方案

### Technologies and Solutions

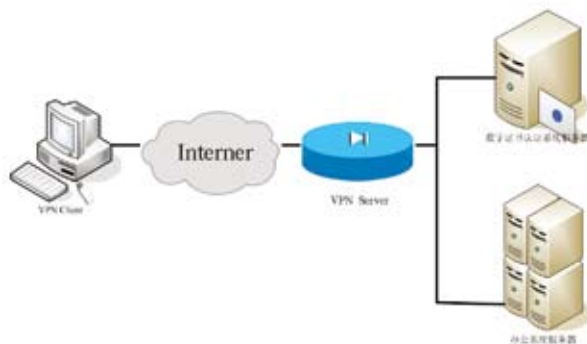
端、支持Office Word文档签章系统。

新华人寿保险公司的安全办公系统：

新华人寿保险公司的安全办公系统由 ePass3000 USB Key的PKI支撑工具包、VPN客户端、VPN服务器、证书认证系统、公文办公系统组成。

新华人寿保险公司及各分支机构员工每人持有一个ePass3000 USB Key，USB Key中保存着此人的X509数字证书及其相关联的私钥。

私钥被物理保护在USB Key中，不能够被他人窃取和修改。员工使用USB Key通过Juniper SSL VPN客户端登录安全办公系统，安全认证系统验证员工的签名来确认员工的身份，并于员工之间建立起安全的数据传输的通道，以确保所传输的数据的机密性和完整性。使处理公文、报表等日常的工作能够在安全的环境下进行，是企业的敏感的信息得到了很好的保护。



飞天诚信ePass3000 USB Key的PKI支撑工具包为PKI及其应用提供了良好的支撑，RSA密钥对保存在USB Key的私密空间，私钥不能够被从USB Key中输出，确保了密钥对的唯一性，也就确保了持有者身份的唯一性。

持有者通过调用消息签名函数，对公文签名，并将签名隐藏在签章图片中，验证者取得持有者的证书，就可以验证此签名了。由于签名是调用持有者私钥，对公文的摘要加密的结果，由于持有者是私钥的唯一的占有者，所以不能够否认他对公文的任何的改动。另外，通过验证公文的摘要可判断公文是否是完整的。

持有者在下载公文时，服务器得到持有者的证书，用户证书中的公钥将加密了公文的密钥加密，并发送给持有者，持有者得到这个经过加密的密钥，由于持有者是私钥的唯一的占有者，所有只有他能够解密而得到这个用来加密公文的密钥，从而解密得到公文的明文。

持有者在上传公文时，先得到服务器的证书，用证书中的公钥将加密了公文的密钥加密，并发送给服务器，服务器得到这个经过加密的密钥，由于服务器是私钥的唯一的占有者，所有只有它能够解密而得到这个用来加密公文的密钥，从而可以解密公文。

持有者登录办公系统时，对办公系统所产生的随机数签名，当办公系统得到这个签名和持有者的证书，如果验证签名和证书都合法，由于持有者是私钥的唯一的占有者，所有就能够确认持有者的身份信息，并为其授权。

持有者的证书被保存在USB Key的公用的空间，以方便多种多样的应用程序读取。提供了良好的接口函数，以方便多种多样的应用程序执行消息签名和验证的功能。提供了良好的接口函数，以方便多种多样的应用程序执行消息加密和解密的功能。

飞天诚信ePass3000 USB Key所提供的这些功能是保障信息安全和访问控制的基础，使新华人寿保险公司的办公系统实现的良好安全性，有效的保护了新华人寿保险公司的信息资源，为安全办公系统成功的运转提供坚固的支撑。