

# USB KEY 构建虚拟专用网 (VPN) 的身份安全和应用安全

## 一、概述

虚拟专用网 (VPN-Virtual Private Network) 指的是在公用网络上建立专用网络的技术。之所以称为虚拟网主要是因为整个 VPN 网络的任意两个节点之间的连接并没有传统专网所需的端到端的物理链路, 而是架构在公用网络服务商所提供的网络平台 (如 Internet, ATM, Frame Relay 等) 之上的逻辑网络, 用户数据在逻辑链路中传输。

由于通过公用网来建立 VPN, 就可以节省大量的通信费用, 而不必投入大量的人力和物力去安装和维护 WAN 设备和远程访问设备; VPN 产品均采用加密及身份验证等安全技术, 保证连接用户的可靠性及传输数据的安全/保密性; 连接方便灵活; 并且 VPN 使用户可以利用 ISP 的设施和服务, 同时又完全掌握着自己网络的控制权。用户只利用 ISP 提供的网络资源, 对于其他的安全设置、网络管理变化可由自己管理。在企业内部也可以自己建立 VPN。因此, VPN 广泛地应用在政府、企事业单位与分支机构内部联网 (Intranet-VPN) 和商业合作伙伴之间的网络互联 (Extranet-VPN)。

随着社会各行业全面的信息化, VPN 建设也如雨后春笋, 由此带来的信息安全也成为了当今不可忽视的课题。为了保证信息安全, 决策者在 VPN 网络建设之初, 常常就会不惜重金花在购买防火墙, 防病毒软件, 等相关的软硬件设施。这一切措施旨在保护信息系统的的核心数据。何谓安全呢, 就是指有相应权限的人员可以接触和操作相应的数据, 任何人无法接触到未被授权给他的数据。然而, 信息系统中的数据终究要为人所用, 如果有人伪造了相应权限人的身份, 那么投入再多的安全防护体系一样形同虚设。因此用户身份认证系统是 VPN 安全体系

的第一道关。

另外在应用中的数据传输, 如何保障数据的完整性和不可否认性, 这也是衡量 VPN 建设成败的关键因素之一。

## 二、USB KEY 的技术介绍

USB Key 的产生不过短短四五年, 这主要是网络的发展, 基于网络的各种应用不断改变着我们的生活, 但由此提出的网上身份安全如何有效识别, 由此诞生了 USB Key, 有效地解决了身份识别的问题。

USB Key 是一种 USB 接口的秘密数据存储设备, 它具有以下特点:

具有硬件 PIN 码保护

每一个 USB Key 都具有硬件 PIN 码保护, PIN 码和硬件构成了用户使用 USB Key 的两个必要因素, 即所谓“双因子认证”。用户只有同时取得了 USB Key 和用户 PIN 码, 才可以登录网上银行系统。即使用户的 PIN 码被泄漏, 只要用户持有的 USB Key 不被盗取, 合法用户的身份就不会被仿冒; 如果用户的 USB Key 遗失, 捡到者由于不知道用户 PIN 码, 也无法仿冒合法用户的身份。

带有安全存储空间

USB Key 具有 8K-64K 的安全数据存储空间, 可以存储数字证书、用户密钥等秘密数据, 对该存储空间的读写操作必须通过程序实现, 用户无法直接读取, 其中用户私钥是不可导出的, 杜绝了复制用户数字证书或身份信息的可能性

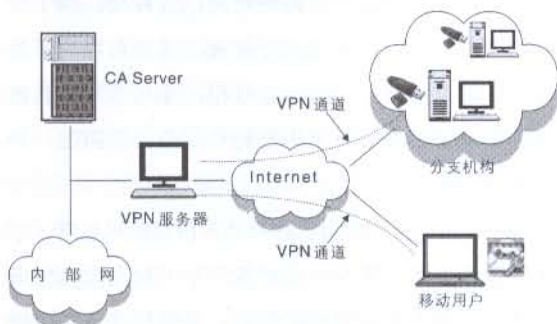
硬件实现加密算法

USB Key 内置 CPU 或智能卡芯片, 可以实现 PKI 体系中使用的数据摘要、数据加解密和签名的各种算法, 加解密运算在 USB Key 内进行, 保证了用户密钥不会出现在计算机内存中, 从而杜绝了用户密钥被黑

客截取的可能性。

北京飞天诚信科技有限公司作为专业生产USB KEY的提供商,公司始终以技术为核心,引领USB KEY的发展,是国内第一个推出USB KEY的厂商,通过几年来的发展和积累,形成了以自主知识产权的高中低端的KEY,几个月前推出了全国第一款32位大容量无驱型高速KEY。使得VPN的构建无论是采用何种认证方式,飞天诚信都有相应的产品满足VPN安全的需要。

### 三、构建虚拟专用网的身份和应用安全



应用拓扑图

使用USB Key构建虚拟专用网主要实现网络终端的身份识别以及实现网络数据交互的完整和不可否认

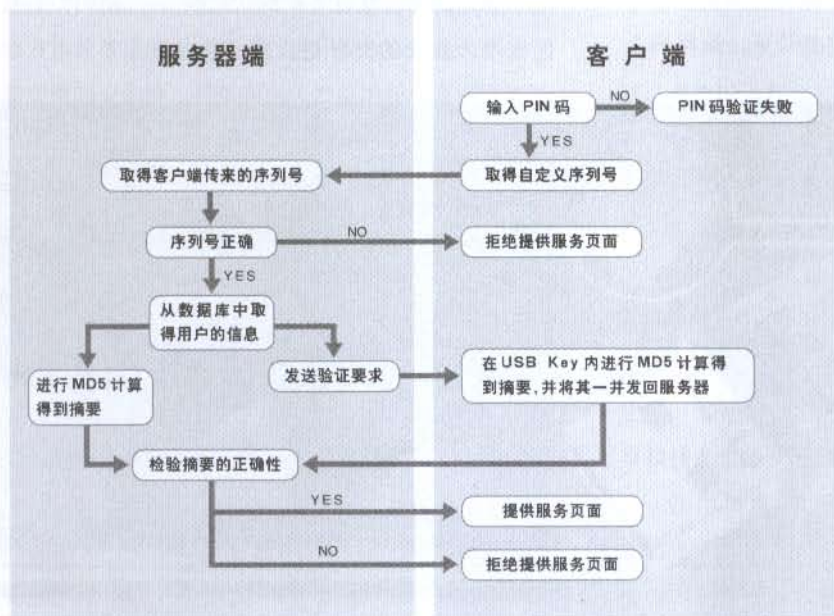
性,有效的保证了数据传输的安全。以下从这两方面阐述。

#### 3.1 身份安全

##### 基于公开密钥体系(PKI)的认证

PKI即Public Key Infrastructure的缩写,也就是所谓“公开密钥体系”,是一种利用现代密码学的公钥密码技术在公开的网络环境中提供数据加密以及数字签名服务的,统一的技术框架。使用公开的密钥算法(也称非对称加密算法)的用户同时拥有匹配的公钥和私钥。私钥由用户保存,且不能泄露,公钥则要广泛公开的发布。私钥无法通过公钥计算获得。公开密钥体系的作用不仅可用于安全密钥交换,还可用于鉴别用户的身份,下面将就如何鉴别用户身份进行描述。

当服务器端需要验证客户端的身份时,服务器端产生一个随机数,发送给客户端,客户端通过USB接口,把随机数R传送入USB KEY中,使用自己的私钥对随机数进行加密,并把加密结果传给服务器端,服务器端通过使用客户的公钥对接收到的加密数据进行解密,对比解密后的数是否和随机数R一致,一致就通过验证。



#### 基于冲击/响应服务的应用

左图为基于冲击响应体制实现强双因子认证流程示意图以及USB Key在网络安全登录拓扑图:

USB Key 认证流程图

当需要在网络上验证用户身份时,先由客户端向服务器发出一个验证请求。服务器接到此请求后生成一个随机数并通过网络传输给客户端(此为冲击)。客户端将收到的随机数通过USB接口提供给USB Key,由USB Key使用该随机数与存储在USB Key中的密钥进行MD5-HMAC运算并得到一个结果作为认证证据传给服务器(此为响应)。与此同时,服务器也使用该随机数与存储在服务器数据库中的该客户密钥进行MD5-HMAC运算,如果服务器的运算结果与客户端传回的响应结果相同,则认为客户端是一个合法用户。

密钥运算分别在USB Key硬件和服务器中运行,不出现在客户端内存中,也不在网络上传输,由于MD5-HMAC算法是一个不可逆的算法,就是知道密钥和运算用随机数就可以得到运算结果,而知道随机数和运算结果却无法计算出密钥,从而保护了密钥的安全,也就保护了用户身份的安全。

### 3.2 应用安全

基于CA认证技术日趋成熟,许多应用中开始使用数字证书进行身份认证与数字加密。数字证书是由权威公正的第三方机构即CA中心签发的,以数字证书为核心的加密技术,可以对网络上传输的信息进行加密和解密、数字签名和签名验证,确保网上

传递信息的机密性、完整性,以及交易实体身份的真实性,签名信息的不可否认性,从而保障网络应用的安全性。

数字证书采用公钥密码体制,即利用一对互相匹配的密钥进行加密、解密。每个用户拥有一把仅为本人所掌握的私有密钥(私钥),用它进行解密和签名;同时拥有一把公共密钥(公钥)并可以对外公开,用于加密和验证签名。当发送一份保密文件时,发送方使用接收方的公钥对数据加密,而接收方则使用自己的私钥解密,这样,信息就可以安全无误地到达目的地了,即使被第三方截获,由于没有相应的私钥,也无法进行解密。通过数字的手段保证加密过程是一个不可逆过程,即只有用私有密钥才能解密。在公开密钥密码体制中,常用的一种是RSA体制。

用户也可以采用自己的私钥对信息加以处理,由于密钥仅为本人所有,这样就产生了别人无法生成的文件,也就形成了数字签名。采用数字签名,能够确认以下两点:

- (1) 保证信息是由签名者自己签名发送的,签名者不能否认或难以否认;
- (2) 保证信息自签发后到收到为止未曾作过任何修改,签发的文件是真实文件。

