

把好电力信息安全系统的第一道关

——飞天 ePass 系列 USB Key 身份认证技术

电力行业是国民经济的基础产业，是关系到国计民生的行业。电力行业的信息化从 60-70 年代开始的电厂自动化监控开始，到现在已经有 30 多年。随着电力行业的不断发展，电力的关键业务不断增长，因此信息化应用也不断增强，网络系统中的应用越来越多。同时，随着 Internet 技术的发展，建立在 Internet 架构上的跨地区、全行业系统内部信息网开始逐步建立，网上应用着各种电力业务及办公系统。显而易见，电力信息网络系统的网络安全问题愈来愈显得重要。

随着电力行业全面的信息化，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电力信息系统的数据安全，所谓安全，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信息安全体系的第一道关。

目前常见的身份认证方式主要有三种，最常见的是使用用户名加口令的方式，当这也是最原始、最不安全的身份确认方式，非常容易由于外部泄漏等原因或通过口令猜测、线路窃听、重放攻击等手段导致合法用户身份被伪造；第二种是生物特征识别技术（包括指纹、声音、手迹、虹膜等），该技术以人体唯一的生物特征为依据，具有很好的安全性和有效性，但实现的技术复杂，技术不成熟，实施成本昂贵，在应用推广中不具有现实意义；第三种也是现在电子政务和电子商务领域最流行的身份方式——基于 USB Key 的身份认证系统。

USB KEY 是结合了现代密码学技术、智能卡技术和 USB 技术的新一代身份认证产品，是一种的秘密数据存储设备，它具有以下特点：

1、双因子认证

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，拾到者由于不知道用户 PIN 码，也无法仿冒合法用户的身份。

2、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。

3、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。支持 RSA, DES, SSF33 和 3DES 算法。

4、便于携带，安全可靠

如拇指般大的 USB Key 非常方便随身携带，并且密钥和证书不可导出，Key 的硬件不可复制，更显安全可靠。

USB Key 身份认证系统的应用方式：

1、基于冲击-响应的双因子认证方式

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提供给 ePass，由 ePass 使用该随机数与存储在 ePass 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 ePass 硬件和服务端中运行，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，就是说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。

2、基于数字证书的认证方式

随着 PKI 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。

PKI 即公共密钥体系，即利用一对互相匹配的密钥进行加密、解密。每个用户拥有一个仅为本人所掌握的私有密钥（私钥），用它进行解密和签名；同时拥有一个公开密钥（公钥）用于文件发送者加密和接收者验证签名。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。

用户也可以采用自己的私钥对信息进行加密，接收者如果用发送者的公钥解密，由于私钥仅为用户本人所有。就能够确认该信息确实是该用户发送的，此过程称之为数字签名。

USB Key 作为数字证书的存储介质，可以保证数字证书不被复制，并可以实现所有数字证书的功能。

USB KEY 在电力企业实现的功能分析：

1. 企业内网

- ☆ Windows 智能卡登陆
- ☆ 企业 OA
- ☆ 文件、硬盘等数据加密
- ☆ 邮件加密
- ☆ 数字签名

2. 电力专网

- ☆ SSL VPN（虚拟专用网）
- ☆ 电子印章
- ☆ 数字证书
- ☆ 数据签名

3. 互联网

- ☆ 网上身份认证
- ☆ 访问安全站点
- ☆ 邮件安全与签名

身份认证技术能够应用于电力企业的多种应用系统，如电力 OA 系统、电力营销业务系统、电力客户服务系统、电力银行联网系统、电力网上营业厅系统等。通过使用身份认证技术不仅使得企业的安全认证得到有效保障，而且极大的提升了企业的管理效率。