 随着计算机、网络、Internet技术的迅猛发展，互联网的影响正逐步渗透到人们生产、生活、工作、学习的各个角落，越来越多的企业、政府机关依托信息网络开展相关的业务活动，如电子商务、电子政务等。由于网络的开放性，不能否认电子商务潜在的安全威胁正慢慢转变为现实。根据国家计算机网络与信息安全管理中心提供的资料，在2001年5月发生的中美黑客大战中，我国有37%的政府网站受到美国黑客攻击，受到了不同程度的损失。根据美国FBI的调查，美国每年因为网络安全造成的经济损失超过170亿美元。 那么对于一个拥有大量会员的专业电子商务网站（例如招投标网站），如何更好的对会员进行管理呢？飞天诚信公司的ePass身份认证锁是一个最佳的解决方案。它不但使会员在网上的交易更加安全，而且，利用ePass的硬件特性，对会员的身份进行确认，从而保障了客户的利益，使得网站安全性得到有效的保障。 飞天ePassND的产品特点1、双因子认证 每一个ePass身份认证锁都具有硬件PIN码保护，PIN码和硬件构成了用户使用身份认证锁的两个必要因素，即所谓“ 双因子认证 ”。用户只有同时取得了锁和用户PIN码，才可以登录商务网平台系统。即使用户的PIN码被泄漏，只要用户持有的认证锁不被盗取，合法用户的身份就不会被仿冒；如果用户的锁遗失，拾到者由于不知道用户PIN码，也无法仿冒合法用户的身份，如果非法使用者输错PIN码次数超过规定的限制，则防盗锁便会处于锁定状态。 2、带有安全存

储空间 ePass身份认证锁具有的安全数据存储空间，可以存储客户的登录信息和密钥等秘密数据，外部应用对其上的存储器所存的数据访问都要通过智能微系统的判定，只有权限相符才允许访问。这样就能实现真正意义上的保护，杜绝了复制客户身份信息的可能性。 3、硬件实现加密算法 ePass身份认证锁内置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，加解密运算在锁内进行，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。 4、便于携带，安全可靠 如拇指般大的ePass认证锁非常方便随身携带，可直接穿到钥匙链上，迎合了追求时尚客户的心里。锁的硬件不可复制，存于ePass认证锁存储器上的数据与对应的硬件进行了绑定加密，即便拆换两只同型号的ePass认证锁存储器也不能正常工作，使用拆片破解的方法也无法复制ePass认证锁内的信息，因此更显安全可靠。 身份认证的优势1、网上身份识别得到有效的保障；2、提高工作效率，降低客户端的应用复杂度；3、信息的不可否认性。 系统建设的目标 通过使用ePassND实现网站登录，达到客户端身份的真实性。通过对客户端权限的设置达到访问资源控制。 实现重要文书的加密传输（例如投标书），以防止信息的泄漏。 系统拓扑图 系统实现的功能 登录功能1、客户登录到电子商务网，插入KEY，选择用户登录；2、提示输入KEY的PIN码；3、PIN码认证通过后，系统自动进行网上身份认证，否则报错。 4、身份认证通过，进行相应业务操作，否则提示身份认证失败信息。 重要文书的加密功能1、初始化KEY，载入登录密钥文件和载入加解密用的密钥文件；2、同时把这两个密钥文件存入数据库中，一

个供登录认证使用，一个供解密客户文书文件（如投标书）使用；3、客户在使用时，点击网站上的“上传文书”，系统将自动调用客户端KEY中的加密用的密钥文件对文书文件进行加密并完成上传；4、对于在解密时，通过解密平台（或解密页面），输入客户名称，服务器端可调出存在数据库中的解密密钥文件对文书文件进行解密。 采购过程的身份认证 对采购类的电子商务网，采购过程的身份认证至关重要。因此可通过ePass身份认证锁来实现采购双方的信任问题。 如果电子商务网对客户数据库有类别的区分，则在ePass认证锁的发放过程中可以相应区分出采购企业，供货企业（设备或服务提供商），对此不同类别的客户可以进行相应权限的设置。在使用中，如何保证采购和供货企业之间身份的真实性？以下就如何实现进行举例阐述。 例如，某企业甲要采购电子商务网中的采购目录中的某个产品，通过浏览采购目录来确定想采购的产品，可通过邮件或者电话进行价格的商议，最终达成共同认可的协议。双方的身份的真实性决定了协议的可靠性。一方通过自己的KEY里的密钥对已确定的协议签名（作一次MD5-HMAC摘要），并附在协议后传给另一方。另一方收到协议和摘要后，将协议上传网站，由网站提取数据库中对方的密钥对协议进行验证签名（作一次MD5-HMAC摘要），并将摘要结果与对方发过来的摘要结果比较，如一致，说明对方的身份是真实的。反之，可对另一方进行认证。 由于每个电子商务的业务模式和商务模式都不尽相同，可根据具体情况设计合适的运营模式，开发出更贴切的运用模式。