解决方案：信息安全平台PowerCA[图] PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/170/2021_2022__E8_A7_A3_E5_86_B3_E6_96_B9_E6_c40_170887.htm 信息安全的解决之道 在电子商务中，越来越多的商业活动是在互未谋面的实体或个人之间进行的，因此客户和商家或者客户和客户之间就存在着相互的身份认证问题。这时候，客户的问题往往是"谁能证明你就是…?"。所以，需要一个客户和商家都信任的权威机构来证明他们各自的身份，就像在现实生活中，人们需要公安局来证明他们的真实身份一样；在电子世界中，我们需要一个"公安局"这样的权威机构来帮助完成交易双方的身份认证。 在现实生活中，您出国考察，需要到工作单位开一张介绍信，证明自己的身份和出国目的，然后得到所去国家的权威机构的签证。在电子世界中，我们同样需要"所在国家的权威机构"开这张"签证"，它能证明我们在电子商务世界中的身份和交易内容；这个"机构"就是权威认证机构CA，这张"签证"就是数字证书或者说是电子签证。 身份识别完成后，是不是问题就全部解决了呢？回答是否定的。怎么证明交易的有效性呢？客户的商业机密同样重要，怎么保护呢？ 所以，企业之间或企业内部的全面完整的信息安全需要： 身份识别 访问控制 数据保密 数据完整 防止否认与防止伪装 安全审计与安全管理 开放网络上的电子商务要求为信息安全提供有效的、可靠的保护机制。这些机制必须提供机密性、身份验证特性(使交易的每一方都可以确认其它各方的身份)、不可否认性(交易的各方不可否认它们的参与)。这就需要依靠一个可靠的第三方机构来验证，而认证中心（CA，Certification

Authority）专门提供这种服务。 证书机制是目前被广泛采用的一种安全机制，使用证书机制的前提是建立CA（Certification Authority --认证中心）以及配套的RA（Registration Authority_注册审批机构）系统。 CA中心，又称为数字证书认证中心，作为电子商务交易中受信任的第三方，专门解决公钥体系中公钥的合法性问题。CA中心为每个使用公开密钥的用户发放一个数字证书，数字证书的作用是证明证书中列出的用户名称与证书中列出的公开密钥相对应。CA中心的数字签名使得攻击者不能伪造和篡改数字证书。认证中心的数字证书，通过运用对称、非对称密码体制，及数字签名、数字信封等密码技术建立起一套严密的身份认证系统（身份识别）和资源访问和权限控制系统（访问控制），以确保电子交易顺利、安全地进行。从而使信息除发送方和接收方外，不被其他人知悉（安全性，数据加密）；传输过程中不被篡改（数据完整）；发送方能确信接收方不是假冒的（不可伪装）；发送方不能否认自己的发送行为（防止否认，不可抵赖性）。 在数字证书认证的过程中，证书认证中心（CA）作为权威的、公正的、可信赖的第三方，其作用是至关重要的。认证中心就是一个负责发放和管理数字证书的权威机构。同样CA允许管理员撤销发放的数字证书,在证书废止列表(CR)中添加新项并周期性地发布这一数字签名的CR。具体地说，CA有4大职能：证书发放、证书更新、证书撤销和证书验证。 RA（Registration Authority），数字证书注册审批机构。RA系统是CA的证书发放、管理的延伸。它负责证书申请者的信息录入、审核以及证书发放等工作（安全审计）。同时，对发放的证书完成相应的管理功能（安全管理

）。RA系统是整个CA中心得以正常运营不可缺少的一部分。RA在PowerCA中涵盖证书审核中心和证书签发中心，它们是以客户程序的方式提供给系统的审核员和系统的管理员。PowerCA实现的功能 实现能够面对面发放高强度的符合X.509国际标准的数字证书；能够为数字证书的用户验证证书的合法性和有效性；能够按照预定的安全规则，或用户的要求，回收并作废用户的数字证书，并将回收作废的数字证书加以保存，以产生回收列表；用户私钥和证书允许保存在Skey或其他存储介质中，实现用户证书的安全存放；实现用户证书和回收列表的网上查询功能；实现网上申请数字证书；实现网上审核证书申请；实现网上签发数字证书；确保PowerCA系统自身的安全性。 PowerCA由七个子系统构成，分别为证书申请中心、证书审核中心、证书签发中心、证书查询中心、证书回收子系统、安全子系统和备份子系统。PowerCA的这七个子系统对应与一般CA认证中心具有的七个分支，各部分的连接如下图所示：证书申请中心的功能是： 面对面产生数字证书请求，审核员使用证书服务主页提供的高级申请将用户的请求文件（用户使用第三方工具形成请求文件）转化为PowerCA识别的用户申请；支持网上申请证书，用户可以在 Internet 上通过浏览器（ IE、Netscape ）连接登录到Web站点申请数字证书。 证书审核中心的功能是： 面对面审核面对面的数字证书请求，按照 PowerCA 的安全策略，审核员接受用户的面对面的证书申请，等待管理员为之签发数字证书；或者拒绝审核用户的面对面的证书申请；支持网上审核用户申请，用户可以在 Internet 上通过"PowerCA证书审核中心"软件连接登录到证书服务器审核用户的数字证书申请

，PowerCA审核员可以利用此子系统审核用户请求；按照PowerCA 的安全策略，审核员接受用户的网上申请，等待管理员为之签发数字证书；或者拒绝审核用户的网上申请。证书签发中心的功能是： 面对面签发面对面的数字证书请求，按照 PowerCA 的安全策略，管理员签发用户的面对面的证书申请；或者拒绝签发用户的面对面的证书申请； 支持网上签发用户申请，用户可以在 Internet 上通过"PowerCA证书签发中心"软件连接登录到证书服务器签发用户的数字证书申请，PowerCA管理员可以利用此子系统签发用户请求；按照PowerCA 的安全策略，管理员接受用户的网上申请为之签发数字证书；或者拒绝签发用户的网上申请。 证书回收子系统的功能是： 用户可以通过向管理员发出签名邮件请求吊销其数字证书，管理员验证用户的签名后，回收用户的数字证书；维护PowerCA的回收列表。 