

登录认证及鉴别授权解决方案

在网络环境下，单位内部的各种信息基础设施越来越多，包括服务器资源、计算机终端、计算机外设、应用程序和网络等各种企业资源的合理分配和使用越来越重要，而分散的身份认证和授权管理让管理员疲于应付，并且容易遗留安全漏洞，不利于统一管理。

此外，使用常规的用户名/口令认证方式，安全上比较脆弱，给管理和统一授权以及责任认定带来极大的不便，容易造成管理漏洞，带来安全隐患。因此，内部必须建立统一管理的高强度的身份认证和授权管理系统，由网络管理人员对内部用户进行统一管理。

● 安全风险分析：

- 1) 内部主机和服务器的访问一般都是基于用户名/口令认证机制，具有一定的脆弱性，容易冒充和伪造。
- 2) 计算机的使用难以控制，经常发生不同部门计算机串用的情况，需要增强对计算机的授权使用；
- 3) 单位内部各类信息资源，包括外设、网络和应用系统等资源的使用无法进行授权管理，容易造成资源浪费，也容易造成管理漏洞。

● 解决方案：

中安网脉(北京)技术股份有限公司研制的中安源可信网络安全平台系统为用户身份管理及统一认证授权提供了完整的解决方案。

- 1) 利用安全证书认证等技术，提高网络用户的可信安全管理，防止非法用户进入网络或内部主机进行非法活动；
- 2) 使用 USB 令牌、指纹识别器等作为内部用户身份标识，支持用户注册、挂起、授权和注销等整个生命周期的用户集中管理；
- 3) 提供基于 Windows 系统增强的认证，可以对计算机的使用权限进行集中授权，只有被授权的用户才能够登录指定的计算机；
- 4) 可以对各种类型的计算机外设进行授权，根据不同用户和不同的计算

机设置不同的权限;

- 5) 可以对各种应用程序的使用进行授权, 根据不同用户和不同的计算机设置不同的权限;
- 6) 可以对各种网络应用协议、网络地址和网络端口等进行授权, 根据不同用户和不同的计算机设置不同的权限;
- 7) 可以对打印设备、移动存储介质的使用以及文件操作权限等进行授权;

● 系统部署示意图:

