电力信息化系统

安盟身份认证解决方案

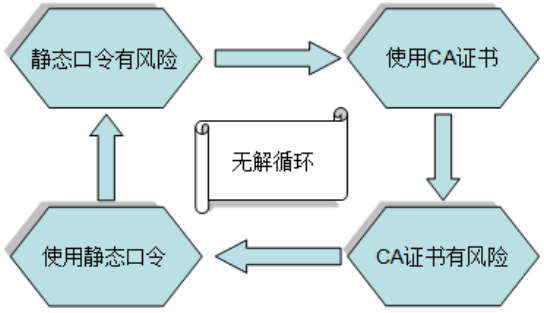
电力信息系统现状

近年来，重大网络安全事件频发，从 CA 证书盗用，到某国际知名动态口令公司种子库失窃，再到多个国内知名门户网站用户数据泄露，这一系列事件表明，网络攻击的主要方向是获取并冒用合法用户身份。

电力信息化系统主要是由诸如 OA、ERP、CRM 等各类应用系统门户和基础系统、网络设备及安全设备组成，主要采用静态口令进行身份认证，或者采用 CA 证书进行用户身份强化认证。

静态口令是身份认证系统中最常用的用户身份鉴别手段，但是由于静态口令可以被重复使用，且猜解难度较低，静态口令的输入终端可靠性无法保障等因素，造成了静态口令进行身份认证技术存在着巨大风险，同时绝大多数用户习惯将所有口令设置为相同，因此随着各门户网站等第三方数据库信息泄露，跟随着的用户口令泄密也给电力信息化系统造成巨大隐患。

为了弥补静态口令的风险，部分系统引入了 CA 证书的认证方式，这种看似记忆因素+持有因素的认证方式在刚刚推广时受到了很大好评，然而由于 CA 证书载体在使用时需要与操作终端 USB 接口进行实际的数据交换，因此被木马或后门程序控制的风险极大，为了避免此类风险，CA 证书又加以**静态口令**保护，来防止木马攻击。然而这种折中的方法使整个身份认证体系陷入恶性循环：



建立安全可靠的电力集团信息系统

1、探寻信息系统风险根源

非法人员为了避免承担风险，增加攻击成功率，针对信息系统的攻击一般采取身份冒用的方式，无论是对于静态口令进行暴力猜解，还是针对 CA 证书载体进行后门调用，均是为了获得合法身份进入系统以实现其非法目，此种攻击手段难以审计和追踪，因此要确保信息系统安全，首先必须对登入用户的身份进行有效认证。

2、规划身份鉴别手段

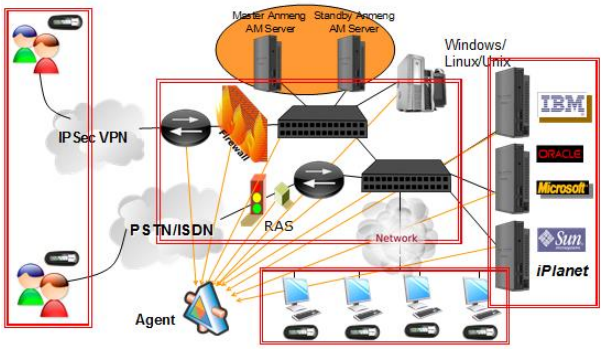
身份认证是信息系统的门户，认证用户身份后，信息系统才能对不同用户进行访问控制和记录。

认证的机制分为两类：简单认证机制和强认证机制。简单的认证中只有名字和口令被服务系统所接受。由于明文的密码在网上传输极容易被窃听截取，一般的解决办法是使用一次性口令（OTP，One-Time Password）机制。

建议使用硬件数字令牌（一次性动态口令）、手机令牌或短信令牌的方式，以确保用户身份能够得到有效认证。

3、建立统一认证管理平台

随着电力信息化系统的进一步建设和完善，OA、ERP、CRM 等系统及各种设备的部署，为了加强信息化系统整体安全性，同时也为了降低投资成本，应在整个信息化系统中对身份认证管理进行资源整合，建立一套安盟身份认证管理系统为后台的身份认证管理平台。



4、安盟认证管理系统平台优势

安盟身份认证管理系统整合了安盟公司多年部署实施身份认证系统的经验及国际主流身份认证技术。由安盟认证服务器、安盟认证代理及安盟令牌三部分组成。

安盟认证服务器采用了服务集群及独立数据库等多项先进技术，为用户提供了一种高效、安全的身份认证管理平台。

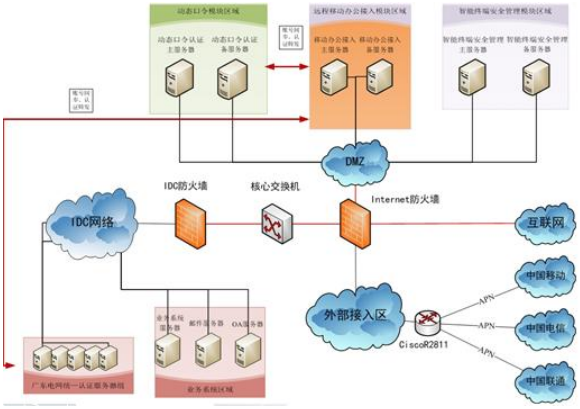
安盟认证代理支持多种认证协议和认证终端，能够为桌面办公终端、VPN、信息化系统应用、服务器及网络设备和安全设备等提供身份认证服务，保护整个信息化平台免受身份冒用的威胁。

安盟认证令牌支持包括硬件、软件、手机、短信等多种形式，同时还能够支持矩阵卡、刮刮卡、挑战应答卡等多种一次性口令产品，为用户提供多种选择，能够充分提升整个信息系统身份认证方面的管理效率。

5、应用方案

密码策略：采用了安盟认证令牌的用户，其完整密码为 PIN 码+令牌码，可以由 PIN 码匹配整体密码规则中的复杂度要求，由令牌码匹配整体密码规则中的密码周期规则，以使整个密码具有极高的安全性，同时避免由于频繁更换密码造成的遗失或书面记录密码的风险。

移动办公：对于逐渐普及的移动终端办公，包括智能手机、平板电脑及笔记本电脑等，由于无法控制办公人员的实际环境，因此对于此类办公环境更加需要强化用户身份认证。



信息化办公系统门户：逐步集成到信息门户中的办公、生产信息系统在电力企业中处于至关重要的位置，门户的安全直接关系到办公、内部管理甚至生产信息网络的安全，一旦系统门户遭遇身份冒用，后果不堪设想，因此需要对系统门户的登录用户进行强化身份认证。