PKI 系统的组成

一个典型的 PKI 系统包括 PKI 策略、软硬件系统、证书机构 CA、注册机构 RA、证书发布系统和 PKI 应用等。

PKI 安全策略

建立和定义了一个组织信息安全方面的指导方针,同时也定义了密码系统使用的处理方法和原则。它包括一个组织怎样处理密钥和有价值的信息,根据风险的级别定义安全控制的级别。

证书机构 CA

证书机构 CA 是 PKI 的信任基础,它管理公钥的整个生命周期,其作用包括:发放证书、规定证书的有效期和通过发布证书废除列表(CRL)确保必要时可以废除证书。

注册机构 RA

注册机构 RA 提供用户和 CA 之间的一个接口,它获取并认证用户的身份,向 CA 提出证书请求。它主要完成收集用户信息和确认用户身份的功能。这里指的用户,是指将要向认证中心(即 CA)申请数字证书的客户,可以是个人,也可以是集团或团体、某政府机构等。注册管理一般由一个独立的注册机构(即 RA)来承担。它接受用户的注册申请,审查用户的申请资格,并决定是否同意 CA 给其签发数字证书。注册机构并不给用户签发证书,而只是对用户进行资格审查。因此,RA 可以设置在直接面对客户的业务部门,如银行的营业部、机构认识部门等。当然,对于一个规模较小的 PKI 应用系统来说,可把注册管理的职能由认证中心 CA 来完成,而不设立独立运行的 RA。但这并不是取消了 PKI 的注册功

能，而只是将其作为 CA 的一项功能而已。PKI 国际标准推荐由一个独立的 RA 来完成注册管理的任务，可以增强应用系统的安全。

证书发布系统

证书发布系统负责证书的发放，如可以通过用户自己，或是通过目录服务器发放。目录服务器可以是一个组织中现存的，也可以是 PKI 方案中提供的。

PKI 的应用

PKI 的应用非常广泛，包括应用在 web 服务器和浏览器之间的通信、电子邮件、电子数据交换(EDI)、在 Intenet 上的信用卡交易和虚拟私有网(VPN)等。

通常来说，CA 是证书的签发机构，它是 PKI 的核心。众所周知，构建密码服务系统的核心内容是如何实现密钥管理。公钥体制涉及一对密钥(即私钥和公钥)，私钥只由用户独立掌握，无须在网上传输，而公钥则是公开的，需要在网上传送，故公钥体制的密钥管理主要是针对公钥的管理问题，目前较好的方案是数字证书机制。