规划和建设烟草行业PKI/CA认证体系

黄云海

【摘　要】本文从烟草行业业务系统的实际需求出发，对规划和建设烟草行业PKI/CA认证体系的必要性及可行性进行了分析，提出了PKI/CA认证是保障烟草行业电子商务、电子政务等各项信息系统安全的一项基础设施。文中对PKI/CA认证技术做了简要介绍，并对目前市场上主流的三种建设模式的优缺点进行了分析，结合行业应用系统的实际情况和行业自身的特点，提出烟草行业PKI/CA体系应采用完全自建的模式，并采用多级结构的方式。文中最后对规划、实施和推广过程中存在的主要问题进行了简要分析。

1　规划和建设烟草行业PKI/CA认证体系

随着烟草行业信息化建设的不断推进，行业卷烟生产经营决策管理系统、电子政务系统、交易系统、资金结算系统等关键业务信息系统纷纷投入使用，对信息内容的安全及签名和交易的安全提出了更高的要求。这些安全问题，需要采用先进的安全技术对网上信息的发送方、接收方进行身份确认，以保证各方信息传递的安全性、完整性、可靠性，以及交易和签名的不可抵赖性。

PKI/CA(公钥基础设施/认证中心)作为一种建立在密码技术基础上的信息安全技术和安全体系架构，是目前唯一能够同时解决身份认证、访问控制、信息保密和抗抵赖的安全技术，是保证电子商务、电子政务、网上核心业务的权威性、可信任性的关键技术。

2　规划和建设行业PKI/CA认证体系的必要性

目前各地、各个核心应用为满足各自的业务需求，纷纷在行业内建立不同安全级别、不同技术基础的认证中心，对于整个烟草行业来说，这将会在信息化建设工作上引发新的混乱：各自CA对于贯穿行业的垂直应用系统，没有权威性，在行业信息系统内部形成天然的隔离，系统重复建设、资源浪费，同时小规模投资的关键应用有可能又放弃采用CA体系，在未来的系统建设中，信息工作的主管部门难以实现对信息平台的统一管理。

按照国家局提出的行业信息化建设“统一平台、统一数据库、统一网络”的要求，为保证整个烟草行业认证系统的权威性、统一性和高度安全性，应该从整体上对行业PKI/CA认证体系建设进行统一规划、严格控制和规范管理，以适应各种应用系统的安全需求。

3　PKI/CA系统

PKI/CA体系采用非对称密钥体系，通过一个证书签发中心(CA)为每个用户和服务器(如WEB服务器等)颁发证书，之后，用户和服务器、用户和用户之间通过证书相互验证对方的合法性。这个过程对于用户是透明的，而且是与具体应用无关的，满足了把用户管理和具体应用分离的需求。

1．PKI/CA体系的组成

PKI由多种功能组成，其中核心部分是具有权威性、可信任性和公正性的第三方认证机构——CA(Certificate Authority)。从PKI总体架构来看，PKI主要由最终用户、认证中心CA系统和注册机构RA系统组成。从应用来看，是基于证书的应用。

(1)认证机构CA

认证机构一般称为CA，在业界通常称为认证中心。它是数字证书的签发机构。PKI系统的关键问题是如何实现密钥管理，公钥机制涉及到一对密钥，即公钥和私钥，私钥只能由证书持有者秘密掌握，无需在网上传输；而公钥体制的密钥管理主要是公钥的管理问题，目前较好的解决方案是引进证书机制。证书是公开密钥体制的一种密钥管理媒介。因此，在公钥体制的环境中，必须有一个可信任的机构对任何一个主体的公钥进行公证，证明主体的身份以及它与公钥的匹配关系。

其中最为重要的是CA自己的一对密钥管理，它必须确保其高度的机密性，防止他方伪造证书。这也就是为何要求权威的数字认证中心须符合国家密码相关政策规定，以及要求建立符合国际标准数据中心的原因。

(2)注册机构RA

CA中心是制证机关，那么为用户发放这些证书的发证机关即是注册中心——RA，它必须保证：1)自身密钥的管理，包括加密密钥及签名密钥的保存、使用、更新和销毁；2)审核用户信息，对申请注册的用户证书信息进行审核、审计，保证相应的人员授权于相应权限；3)登记黑名单，对过期的证书及因各种原因而撤消的证书及时登记并向CA中心发送，以确保CRL(证书废止列表)的及时更新，并对CRL进行管理

注册中心是直接面向于用户的。制证中心负责审核证书申请者的真实身份，审核通过后，由制证中心完成制证过程。所以RA具有发证授权的权威性，而制证中心则相当于提供技术支持、维护整个制证加工厂的厂商。

2．PKI技术与其它身份认证技术对比

PKI技术具有功能全面、高度安全、成熟可靠的特点，整体综合能力是最全面和最强大的，可以满足应用安全各个方面的需求，以下是PKI技术与其它技术的对比：

功能	PKI技术	用户名/口令技术	动态口令技术	生物特征技术
身份认证安全性	高	低，口令容易被猜测和盗取	中	中
身份认证范围	用户与服务器互相认证	只认证用户	只认证用户	只认证用户
信息保密性(加密)	可以实现	不能实现	不能实现	不能实现
信息完整性(防篡改)	可以实现	不能实现	不能实现	不能实现
防止否认	可以实现	不能实现	不能实现	不能实现
技术可靠性	高	高	高	不高，由于识别技术的限制，会出现特征识别错误
可扩展性	高，数字证书可以在任何应用系统中得到认证而不依赖于集中的服务器	低，需要集中的认证服务器(用户口令库)	低，需要集中的动态口令认证服务器	低，需要集中的认证服务器(用户特征库)
标准化程度	高，具有众多相关国际标准	低，用户或厂商自行开发	低，用户或厂商自行开发	低，用户或厂商自行开发
管理与维护难度	中，可以不集中维护用户的密钥(私钥)	较高，需要集中维护大量的用户口令数据	高，用户的硬件设备需要定期更换，为用户和管理员造成负担	高，需要对用户的生物特征一一采样并维护，一旦发生变化，还需要重新采样
大用户量下的整体投资	中	低	高，用户口令硬件设备昂贵	高，用户生物特征识别设备昂贵

4　烟草行业PKI/CA认证体系可行性分析

烟草行业PKI/CA认证系统的建设应以信息安全为基础，以业务应用为核心，遵循国家有关法律法规，统一规划、统一标准，为烟草行业信息的基础设施和对外信息服务提供以PKI/CA技术为基础的认证系统。

(1)建设环境的可行性

各级单位，各业务系统，特别是电子商务、电子政务系统的建设，对建立CA认证体系的要求迫切，是需求在强烈呼唤CA体系的建设，许多省级局(公司)都在等待国家局CA体系规划的出台和实施，因此CA体系建设具有良好的环境。

(2)技术上的可行性

自二十世纪九十年代初期以来，作为电子商务信息安全的关键和基础性技术的PKI逐步得到了许多国家的政府和企业的广泛重视，PKI技术由理论研究进入到商业化应用阶段。IETF、ISO等机构陆续颁布了X.509、PKIX、等PKI应用相关标准。一些大的IT厂商，如Microsoft、Novel、Sun等都开始在自己的网络基础设施产品中支持PKI功能。

(3)政策法律上的可行性

2004年8月28日，第十届全国人民代表大会常务委员会第十一次会议通过了中华人民共和国电子签名法；2005年1月28日，中华人民共和国信息产业部第十二次部务会议审议通过了《电子认证服务管理办法》。

(4)实施上的可行性

由于技术上的可行，使得我们在实施规划和建设CA体系时，可以寻找适宜的方式和成熟的产品。另外，经过多年的信息化建设，行业网络初具规模，安全体系逐渐建立起来，也有一支比较有经验和能力的技术队伍，为建立和管理CA系统创造了必要的条件。

5　规划和建设行业PKI/CA认证体系

规划和建设行业PKI/CA认证体系，需要根据烟草行业的实际情况，统一进行认证体系结构设计，并确定行业PKI/CA认证体系的运行管理规范、部署策略、实施原则，及各级CA和RA中心建设的技术规范。

1．烟草行业PKI/CA体系建设模式的选择

烟草行业要建立自己的PKI/CA系统，就面临着多种建设方式的选择，建设方式的选择直接关系到了PKI/CA系统的使用、管理、维护以及PKI/CA系统为行业各项业务系统提供安全平台的安全程度。从当前国内PKI/CA体系发展的情况看，行业CA体系的建设模式可从下面三种方式中进行选择：

(1)采用国内已有面向公众服务的商业性数字认证机构模式

采用社会上的认证中心，在短期应用，系统需要少量证书的情况下，前期建设成本较低，无需建立维护、培训和支持团队，无需自己定义管理和安全策略。但这种做法更适合单一业务或分散的没有关联业务应用。采用社会上的认证中心后，信息化建设在很多方面都比较被动，缺少应用和管理的自主灵活性。证书管理策略依赖于服务商，业务可靠性、稳定性依赖于外部服务，风险较高。长期来看，采用社会上的认证系统购买服务投入较大，成本较高。

(2)完全自行建设模式

购买一整套PKI软件，然后建立一整套相关的服务体系。

这种模式下，我们要参予建立、维护、培训和运营的整个PKI过程，并对PKI所有事物负全责，其中包括系统、通信、数据库、以及物理安全、网络安全配置、高可靠的冗余系统、灾难恢复等，对人员管理要求也比较高。这种模式下，系统建设初期成本较高，同时需建立自主维护、培训和支持的人员，需要信息主管部门要设计规范管理和安全策略。但从长期来看，自行建设行业自己的认证体系，更易于针对行业内应用进行定制，从而更好的配合行业内部的业务系统管理模式。同时完全自主管理，在长期运行，发放大批量证书的情况下更节省费用；更适合具有全国、全省范围内有多种业务相关的关键信息系统的应用。

(3)基于服务的托管自建模式

这是一种介于上述两种模式中间的一种方式，是指客户配置一套集成的PKI软件，在客户本地建设面向最终用户的系统前台——证书注册中心(RA中心)，直接利用第三方PKI服务提供商的CA服务，作为系统的核心后台——认证中心(CA中心)，共同为最终用户提供安全认证服务。

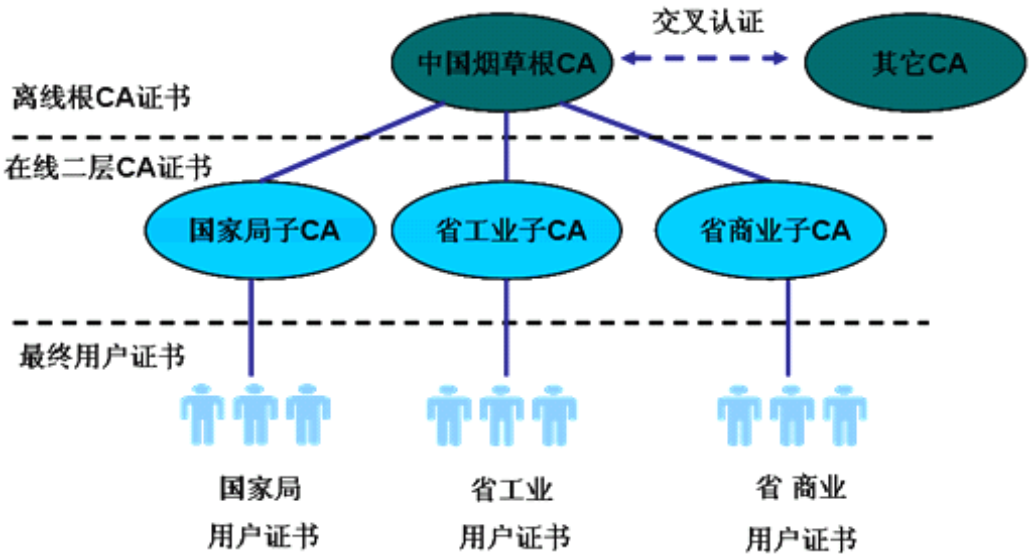
尽管关键设备托管在外部，但不同于第一种模式，它仍然是烟草行业建立的自己的PKI/CA体系，烟草行业的根CA证书是使用国家局自己的加密卡产生并自签的根CA证书，国家局只需通过驻留在烟草内部的前台系统对后台的烟草PKI进行远程控制、监管来对用户提供证书生命周期的各项服务。在这种模式下，复杂、专业的PKI核心服务、维护工作和安全保障交由托管的数字认证中心完成，国家局不需更多的专业人员，只需要对其内部相关人员进行简单培训即可，国家局不需承担由数字认证中心带来的任何技术风险。但是，由于提供托管服务的商业中心数目非常少，可以选择的余地不大。

从初步调研并结合行业应用系统的实际情况和行业自身的特点，烟草行业PKI/CA体系建设的模式建议采用完全自建的模式，并按照“全行业统一规划，试点建设和应用，再全面推广”的策略分步实施。通过建立合理的PKI/CA体系，为烟草行业网站系统建立可行、实用、可靠并且扩展性很强的用户认证管理机制。

2．烟草行业PKI/CA体系的结构

根据烟草行业各级单位比较多，及行业垂直管理的特点，为了保证认证系统的安全性、可靠性、高效性、可扩展性，烟草

行业CA体系应设计为多级结构，至少包括一个根CA和多个二级CA(子CA)。体系结构如下图所示：



（1）根CA

烟草行业PKI/CA认证体系必须建立一个根CA，它负责签发和管理整个认证体系的各级CA的证书、制定和审批总体政策、并与其它的根CA进行交叉认证并制定具体政策、管理制度和运作规范等。

为保证根CA的安全，CA认证体系中的根CA设计为离线操作，该CA无需频繁发证，仅在签发下级CA证书时开启，信息和文件（申请书、证书、CRL）的传递以离线形式操作。

（2）二级CA（子CA）

二级CA指国家局子CA，各省级局（公司）、各省工业公司的CA，其证书由根CA签发，负责最终用户证书的申请和签发、最终用户证书的冻结和解冻、最终用户证书的作废、最终用户证书的更新和查询、证书管理事件的审计、发布最终用户证书和证书废止列表(CRL)，以及其它的辅助功能。国家局的子CA是国家局在线的运营CA。

二级CA需要经常发证并且需要迅速响应，所以二级CA必须在线操作。证书和CRL分布于一个支持LDAP协议标准的目录服务器中。证书和CRL的查询通过LDAP协议实现。

PKI/CA体系采用LDAP目录技术管理用户。LDAP(Lightweight Directory Access Protocol)是目录服务在TCP/IP上的实现（RFC 1777 V2版和RFC 2251 V3版）。LDAP是对X.500的目录协议的移植，简化了X.500实现方法，称为轻量级的目录服务。

（3）RA中心建设

RA作为CA的注册审核机构，完成证书用户在证书注册申请、证书申请的审核、证书发放、以及后续的证书更新、作废等管理工作。

根据目前烟草行业的管理模式，可在国家局/总公司建设局机关RA，负责国家局机关/总公司工作人员证书的管理；在CA系统建设初期，局机关RA还可以代管部分省的证书管理工作，在这些省的RA建立之后，由这些省级RA接替证书管理工作。

（4）多级结构的优点

多级CA体系，由国家局根CA对各下属CA进行有效的控制，1)保证整个烟草行业的信任体系统一；2)提高了整个CA系统的安全性；3)多级CA系统独立维护和运行，具有很好的灵活性和可扩展性，并且降低了上级CA的工作压力；4)多级CA可以通过灵活的RA体系与不同的应用系统连接，满足不同种类、不同规模的业务需求。

3．规划、实施和推广过程中存在的主要问题

(1)CA系统与应用结合的问题

目前在CA系统和应用系统结合的问题上，通常的做法是使用CA系统来进行认证，而权限的分配则由应用系统来确定，这就涉及CA系统与应用系统结合的二次开发问题，同时为保障证书的有效使用，又要求在证书的使用过程中，认证应紧密嵌入到应用系统中。

(2)已有业务系统的移植问题

由于国家局和行业已先后建立了数十个业务系统，对这些系统的移植要采取循序渐进的办法。

(3)行业CA体系的统一问题

统一规划和管理烟草行业的CA体系建设，对未来行业信息化建设的进一步推进，各系统的互信互联互通非常关键。对于已建立的类似的CA系统要逐步纳入到统一的行业CA体系中来。这主要是一个管理问题，需要制定相应的CA体系管理规范和流程规范。

6　相关术语和缩略词

名　词	解　　释
PKI	Public Key Infrastructure ， 公钥基础设施
CA	Certification Authority ， 认证中心
RA	Registration Authority ， 注册机构
CRL	Certificate Revocation Lists ， 证书废止表 ， 又称黑表
CTN	China Trust Network全国互信网络
SSL	Secure Socket Layer，安全套接层

———————————————

作者简介：黄云海，国家烟草专卖局烟草经济信息中心，电子邮件huangyh@tobacco.gov.cn