ICS 65.160
X 89
备案号:27104—2010

YC

中华人民共和国烟草行业标准

YC/T 327—2009

烟草行业数字证书应用接口规范

Technical specification for digital certificate application interface to tobacco industry

2009-12-14 发布　　2010-03-01 实施

国家烟草专卖局　　发布

目　　次

前　言

本标准的附录A、附录B为资料性附录。

本标准由国家烟草专卖局提出。

本标准由全国烟草标准化技术委员会信息分技术委员会(SAC/TC 144/SC 7)归口。

本标准起草单位:国家烟草专卖局烟草经济信息中心。

本标准主要起草人:张雪峰、王海清、刘东平、轩松岭、张萌、王翊心、李伟。

烟草行业数字证书应用接口规范

1 范围

本标准规定了烟草行业数字证书应用的总体框架与应用规范，描述了烟草行业与证书相关应用的技术要求。

本标准适用于烟草行业与数字证书相关应用的规划、设备招标、方案设计以及业务实施。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 13000.1—1993 信息技术 通用多八位编码字符集(UCS) 第一部分：体系结构与基本多文种平面(idt ISO/IEC 10646-1：1993)

GB/T 16264.2—2008 信息技术 开放系统互连 目录 第2部分：模型(ISO/IEC 9594-2—2005，IDT)

GB/T 16264.8—2005 信息技术 开放系统互连 目录 第8部分：公钥和属性证书框架(ISO/IEC 9594-8：2001，IDT)

GB/T 19713—2005 信息技术 安全技术 公钥基础设施 在线证书状态协议

GB/T 19771—2005 信息技术 安全技术 公钥基础设施 PKI组件最小互操作规范

GB/T 20520—2006 信息安全技术 公钥基础设施 时间戳规范

IETF RFC 2251 轻量级目录访问协议(LDAP V3)

IETF RFC 2246 安全传输层协议 V1.0

3 术语和定义

GB/T 16264.2、GB/T 16264.8、GB/T 19713、GB/T 19771、GB/T 20520、GB/T 13000.1确立的以及下列术语和定义适用于本标准。

3.1

公钥证书 public key certificate

用户的公钥连同其他信息，并由发布该证书的证书认证机构的私钥进行加密使其不可伪造。

[GB/T 16264.8—2005，第3章]。

3.2

证书认证机构 certificate authority；CA

负责创建和分配证书，受用户信任的权威机构。用户可以选择该机构为其创建密钥。

[GB/T 16264.8—2005，第3章]。

3.3

证书撤销列表 certificate revocation list；CRL

一个已标识的列表，它指定了一套证书发布者认为无效的证书。除了普通CRL外，还定义了一些特殊的CRL类型用于覆盖特殊领域的CRL。