ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30277—2013

信息安全技术　公钥基础设施 电子认证机构标识编码规范

Information security technology—Public key infrastructures—Certification authentication institution identity code specification

2013-12-31 发布　　2014-07-15 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准依据 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:国家信息安全工程技术研究中心、上海信息安全工程技术研究中心、北京中油瑞飞信息技术有限责任公司。

本标准主要起草人:袁峰、郭晓雷、袁文恭、杨恒亮、浦雨三、吕增江、黄晟。

引　言

随着我国信息化的发展，全国已经建设了国家根电子认证机构和多种电子认证服务机构。为了方便对电子认证机构的统一管理，实现多数字证书的相互识别，需要每个电子认证机构有一个按照统一规范标准授予的相应代码或对象标识符。但是，目前各个电子认证机构都是自己设定自己的名称及其格式，没有全国统一的规范代码。本标准对我国电子认证机构的标识代码给出了统一规范，以满足信息化建设对不同电子认证机构签发的证书进行辨识的需要。

电子认证机构分为全国性、行业性等多种类型。《电子签名法》发布后，电子认证服务行业明确了主管部门，相应的法律法规逐步完善。目前，已有多家电子认证机构获得运营许可并为相关信息系统提供了证书认证服务，不同电子认证机构签发的证书辨识急需制定统一、规范的标识代码机制。

本标准可用于电子政务、电子商务、行业、企业等多类电子认证机构。

信息安全技术　公钥基础设施
电子认证机构标识编码规范

1　范围

本标准确立了电子认证机构标识代码编制规范的一般原则。

本标准适用于基于 PKI 应用系统，统一的电子认证机构编码为建立全国性的 CA 目录查询提供了基础条件。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 16262.1—2006　信息技术　抽象语法记法一(ASN.1) 第 1 部分：基本记法规范

GB/T 18521　地名分类与类别代码编制规则

GB/T 20518—2006　信息安全技术　公钥基础设施　数字证书格式

GB/T 25069—2010　信息安全技术　术语

GM/T 0006—2012　密码应用标识规范

3　术语和定义

下列术语和定义适用于本文件。

3.1

电子认证机构　certificate authority

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。

3.2

对象标识符　object identifier

系统赋予对象实体的唯一性数字化代码，用以标识对象的身份。

4　缩略语

下列缩略语适用于本文件。

CA：电子认证机构 (Certification Authority)

OID：对象标识符 (Object Identifier)

PKI：公钥基础设施 (Public Key Infrastructure)

5　CA 代码编制方法

5.1　CA 属性分类与约定

CA 系统可从不同角度说明其特性：