ICS 35.040
L 80
备案号：38312—2013

GM

中华人民共和国密码行业标准

GM/T 0014—2012

数字证书认证系统密码协议规范

Digital certificate authentication system cryptography protocol specification

2012-11-22 发布　　2012-11-22 实施

国家密码管理局　　发 布

目　　次

前　言

本标准依据 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准的附录 A、附录 D 为规范性附录，附录 B、附录 C 为资料性附录。

本标准由国家密码管理局提出并归口。

本标准起草单位：上海信息安全工程技术研究中心、国家信息安全工程技术研究中心、上海格尔软件股份有限公司、海泰方圆科技有限公司、北京数字认证股份有限公司。

本标准主要起草人：袁文恭、刘平、郭晓雷、袁峰、李增欣、杨恒亮、谢安明、谭武征、柳增寿、李元正。

引　言

本标准是为我国信息安全基础设施建设中关于数字证书认证系统密码协议提供的规范。本标准描述了证书认证和数字签名中通用的安全协议流程、数据格式和密码函数接口等。安全协议以密码技术为基础，为网络内的数字证书认证系统密码协议提供统一、通用的通联协议服务，以满足网络内的实体对数字证书认证系统的真实性、保密性、完整性、可认证性和不可否认性等安全需求。

本标准凡涉及密码算法相关内容，按照国家有关法规实施。

数字证书认证系统密码协议规范

1 范围

本标准适用于电子政务/电子商务基于密码技术的数字证书认证系统的设计、建设、检测、运营及管理，规范数字证书认证系统中密码协议的标准化应用，推动数字证书认证系统密码协议的互连互通和相互认证。对于组织或机构内部使用的数字证书认证系统密码协议的建设、运营及管理，可参考使用。

同时本标准还可为安全产品生产商提供产品和技术的准确定位和标准化的参考，提高安全产品的可信性和互操作性。

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。凡是注明日期的引用文件，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 16264.8 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

GB/T 19713 信息技术 安全技术 公钥基础设施 在线证书状态协议

GB/T 19714 信息安全 安全技术 公钥基础设施 证书管理协议

GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 25059 信息安全技术 公钥基础设施 简易在线证书状态协议

GM/T 0006 密码应用标识规范

GM/T 0009 SM2密码算法使用规范

GM/T 0010 SM2密码算法加密签名消息语法规范

GM/T 0015 基于SM2密码算法的数字证书格式规范

3 术语和定义

3.1

CA撤销列表 certificate authority revocation list；CARL

标记已经被撤销的CA的公钥证书的列表，表示这些证书已经无效。

3.2

证书认证系统 certificate authentication system

对生存周期内的数字证书进行全过程管理的安全系统。

3.3

证书认证路径 certification path

在目录信息树中对象证书的一个有序的序列。路径的初始节点是最初待验证对象的公钥，可以通过路径获得最终的顶点的公钥。

3.4

证书策略 certificate policy

一个指定的规则集合，它指出证书对于具有普通安全需求的一个特定团体和(或)具体应用类的适