ICS 35.040
L 80
备案号:44635—2014

GM

中华人民共和国密码行业标准

GM/T 0034—2014

基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范

Specifications of cryptograph and related security technology for certification system based on SM2 cryptographic algorithm

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　发布

目　　次

前　言

本标准按照 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。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：上海市数字证书认证中心有限公司、上海格尔软件股份有限公司、北京市数字证书认证中心有限公司、长春吉大正元信息技术股份有限公司、北京海泰方圆科技有限公司、无锡江南信息安全工程技术中心、成都卫士通信息产业股份有限公司、兴唐通信科技有限公司、上海颐东网络信息有限公司、万达信息股份有限公司、飞天诚信科技股份有限公司、北京华大智宝电子系统有限公司、北京握奇智能科技有限公司、山东得安信息技术有限公司、国家信息安全工程技术研究中心、国家密码管理局商用密码检测中心。

本标准起草人：刘平、崔久强、刘承、谭武征、李述胜、赵丽丽、柳增寿、徐强、李元正、王妮娜、夏东山、李海杰、于华章、陈跃、胡俊义、孔凡玉、袁峰、李志伟。

基于SM2密码算法的证书认证系统密码及其相关安全技术规范

1 范围

本标准规定了基于SM2密码算法的数字证书认证系统的密码及相关安全的技术要求，包括证书认证中心，密钥管理中心，密码算法、密码设备及接口等。

本标准适用于指导第三方认证机构的数字证书认证系统的建设和检测评估，规范数字证书认证系统中密码及相关安全技术的应用。非第三方认证机构的数字证书认证系统的建设、运行及管理，可参照本标准。

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 2887 计算机场地通用规范

GB/T 6650 计算机机房用活动地板技术条件

GB/T 9361 计算机场地安全要求

GB 50174 电子信息系统机房设计规范

GM/T 0014 数字证书认证系统密码协议规范

GM/T 0015 基于SM2密码算法的数字证书格式规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0018 密码设备应用接口规范

GM/T 0019 通用密码服务接口规范

GM/T 0020 证书应用综合服务接口规范

BMB 3—1999 处理涉密信息的电磁屏蔽室的技术要求和测试方法

RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)

3 术语和定义

下列术语和定义适用于本文件。

3.1

认证机构证书 authority certificate

签发给证书认证机构的证书。

3.2

CA证书 CA certificate

由一个CA给另一个CA签发的证书，一个CA也可以为自己签发证书，这是一种自签名的证书。

3.3

证书认证系统 certificate authentication system

对数字证书的签发、发布、更新、撤销等数字证书全生命周期进行管理的系统。