ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0095—2020

电子招投标密码应用技术要求

Technical requirements for applications of cryptography in electronic bidding

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：北京数字认证股份有限公司、广州公共资源交易中心、天地融科技股份有限公司、中国电力科学研究院有限公司、上海市数字证书认证中心有限公司、数安时代科技股份有限公司、中金金融认证中心有限公司、杭州天谷信息科技有限公司、吉大正元信息技术股份有限公司。

本文件主要起草人：詹榜华、田景成、杨玉奇、赵兵、林雪焰、李向锋、张永强、蓝虹、郭晓栋、李明、牟宁波、翟峰、程亮、赵丽丽、陈伟毅。

电子招投标密码应用技术要求

1 范围

本文件规定了密码技术在电子招投标业务中的应用技术要求，包括在电子招投标过程中，使用密码算法、密码产品的技术要求。

本文件适用于指导电子招投标系统中密码子系统的设计、实现和使用，电子招投标系统中密码子系统的测试、管理也可参照使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GM/T 0031 安全电子签章密码应用技术规范

GM/T 0054 信息系统密码应用基本要求

GM/Z 4001—2013 密码术语

3 术语和定义

GM/Z 4001—2013 界定的以及下列术语和定义适用本文件。

3.1

非对称密码算法 asymmetric cryptographic algorithm

加解密使用不同密钥的密码算法。其中一个密钥（公钥）可以公开，另一个密钥（私钥）必须保密。由公钥求解私钥在计算上是不可行的。

3.2

数字证书 digital certificate

由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。

注 1：数字证书也称公钥证书。

注 2：按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.3

证书认证机构 certificate authority；CA

对数字证书进行全生命周期管理的实体。

注：证书认证机构也称电子认证服务机构。