ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0120—2022

基于云计算的电子签名服务技术实施指南

Implementation guidance for electronic signature service based on cloud computing

2022-11-20 发布　　2023-06-01 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、中国科学院数据与通信保护研究教育中心、北京天融信网络安全技术有限公司、中电科网络安全科技股份有限公司、三未信安科技股份有限公司、长春吉大正元信息技术股份有限公司、中国电力科学研究院有限公司。

本文件主要起草人：李向锋、林雪焰、张永强、景鸿理、张立廷、傅大鹏、郑昉昱、高志权、赵丽丽、翟峰、刘中。

基于云计算的电子签名服务技术实施指南

1 范围

本文件给出基于云计算的电子签名服务实施可参照的路线和方法。

本文件适用于指导基于云计算的电子签名服务系统的建设和相关产品的开发，对于基于云计算的电子签名服务系统的测试和管理可参照使用。

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 15843.3 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制

GB/T 15843.4 信息技术 安全技术 实体鉴别 第4部分：采用密码校验函数的机制

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 25064 信息安全技术 公钥基础设施 电子签名格式规范

GB/T 25069 信息安全技术 术语

GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 31168 信息安全技术 云计算服务安全能力要求

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 32918.2 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法

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

GB/T 36326 信息技术 云计算 云服务运营通用要求

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 38636 信息安全技术 传输层密码协议(TLCP)

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GM/T 0109—2021 基于云计算的电子签名服务技术要求

GM/Z 4001 密码术语

3 术语和定义

GB/T 25069、GM/T 0109—2021、GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

电子签名 electronic signature

数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

3.2

云计算 cloud computing

通过网络访问可扩展的、灵活的物理或虚拟资源池，并可按需自助获取管理资源的模式。