ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0109—2021

基于云计算的电子签名服务技术要求

Technical requirements for electronic signature service based on cloud computing

2021-10-18 发布　　2022-05-01 实施

国家密码管理局　　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　基于云计算的电子签名服务一般架构 …… 2
5.1　架构模型 …… 2
5.2　服务模式 …… 3
6　依赖方技术要求 …… 3
7　签名方技术要求 …… 4
7.1　总体要求 …… 4
7.2　本地数据保护 …… 4
7.3　身份鉴别 …… 4
7.4　通信数据保护 …… 4
7.5　密钥管理 …… 4
7.6　电子签名的确认与控制 …… 4
8　云签名服务技术要求 …… 4
8.1　概述 …… 4
8.2　建设要求 …… 4
8.3　电子签名服务要求 …… 5
8.4　运行支撑要求 …… 8
8.5　安全审计要求 …… 8
附录 A(资料性)　几种典型的云签名服务模式 …… 10

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。

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、数安时代科技股份有限公司、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、中金金融认证中心有限公司、中国电力科学研究院有限公司、北京金奥博数码信息技术有限责任公司、杭州天谷信息科技有限公司、浙江汇信科技有限公司、北京国富安电子商务认证有限公司、江苏意源科技有限公司。

本文件主要起草人：李向锋、林雪焰、张永强、傅大鹏、田景成、高志权、赵丽丽、谢吉华、翟峰、王新华、张翼、程亮、王忠义、杨洋、徐冠宁、王胜男。

引　言

近年来，在移动互联网和云计算等新技术的推动下，很多应用领域从业务模式到技术支撑，都发生了深刻的变化，业务越来越需要能够随时、随地开展和确认，而为保障业务合规性和安全性的电子签名技术，也应该及时适应这些变化，在这些新的场景中发挥积极作用。同时，移动互联网业务中，通过电子签名技术保证业务安全性的需求越来越多，电子签名相关应用将向移动互联网延伸。

基于云计算的电子签名，是为业务提供电子签名功能的一种方式。服务方将电子签名以云服务形式提供给用户，使用户能够方便、低成本、随时随地生成各类业务所需的，具有法律效力的电子签名。通过制定本文件，能够对基于云计算的电子签名服务进行规范，从而为业务系统提供便捷可靠的电子签名能力支撑。

基于云计算的电子签名服务技术要求

1 范围

本文件描述了基于云计算的电子签名服务密码技术需求，提出了采用数字证书和数字签名技术实现的基于云计算的电子签名服务的密码技术要求。

本文件适用于指导基于云计算的电子签名服务的建设、管理、检测和应用。

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 信息技术 安全技术 实体鉴别

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 22239 信息安全技术 网络安全等级保护基本要求

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 25064 信息安全技术 公钥基础设施 电子签名格式规范

GB/T 31168—2014 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(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

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—2021 信息安全技术 信息系统密码应用基本要求

GM/Z 4001 密码术语

3 术语和定义

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。

注：本文件中特指采用数字证书和数字签名技术实现的电子签名。

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，并可按需自助获取与管理资源的模式。