ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0104—2021

云服务器密码机技术规范

Specifications of cloud host cryptographic server

2021-10-18 发布　　2022-05-01 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。。

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：成都卫士通信息产业股份公司、四川大学、山东得安信息技术有限公司、北京三未信安科技发展有限公司、北京江南天安科技有限公司、北京海泰方圆科技股份有限公司、格尔软件股份有限公司、中国科学院数据与通信保护研究教育中心、兴唐科技通信有限公司、无锡江南信息安全工程技术中心、北京数字认证股份有限公司。

本文件主要起草人：罗俊、龚勋、董贵山、吴庆国、张立廷、李川、宋飞、马洪富、高志权、李国、马晓艳、柳晶、蒋红宇、郑强、梁乐、曹硕、王伟、徐明翼、赵松。

云服务器密码机技术规范

1 范围

本文件定义了云服务器密码机的相关术语，规定了云服务器密码机的总体结构、功能要求、硬件要求、软件要求、安全性要求和检测要求等有关内容。

本文件适用于云服务器密码机的研制、使用，也可用于指导云服务器密码机的检测。

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 9813.3—2017 计算机通用规范 第3部分：服务器

GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

GB/T 32915—2016 信息安全技术 二元序列随机性检测规范

GB/T 35293—2017 信息技术 云计算 虚拟机管理通用要求

GB/T 36322—2018 信息安全技术 密码设备应用接口规范

GB/T 37092—2018 信息安全技术 密码模块安全要求

GB/T 36968—2018 信息安全技术 IPSec VPN 技术规范

GB/T 38636—2020 信息安全技术 传输层密码协议(TLCP)

GB/T 38625—2020 信息安全技术 密码模块安全检测要求

GM/T 0030—2014 服务器密码机技术规范

GM/T 0062—2018 密码产品随机数检测要求

GM/T 0088—2020 云服务器密码机管理接口规范

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

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，并可按需自助获取和管理资源的模式。

3.2

云服务器密码机 cloud-hosted hardware security module(CHSM)/ cloud cryptographic server

在云计算环境下，采用虚拟化技术，以网络形式，为多个租户的应用系统提供密码服务的服务器密码机。

3.3

宿主机 host

为虚拟密码机提供运行环境和硬件资源的物理设备，同一台宿主机内的多个虚拟密码机共享该宿