ICS 35.040
CCS L 80

中华人民共和国密码行业标准

GM/T 0088—2020

云服务器密码机管理接口规范

Cloud cryptographic server management interface specification

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：北京江南天安科技有限公司、阿里云计算有限公司、北京三未信安科技发展有限公司、新飞凡（上海）云计算服务有限公司、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、中国科学院数据与通信研究教育保护中心。

本文件主要起草人：李国、胡杰、马晓艳、张钊、苏建东、杨李贝、高志权、吕鹏啸、罗俊、吴庆国、徐明翼、张超、梁乐、王伟、曹硕。

云服务器密码机管理接口规范

1 范围

本文件规定了云平台管理系统与云服务器密码机之间的设备管理接口和协议。

本文件适用于云服务器密码机的研制和检测，也适用于云平台管理系统的开发和使用。

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 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 35276 信息安全技术 SM2 密码算法使用规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

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密码设备。

3.2

虚拟密码机 virtual security module（VSM）；virtual cryptographic server

云服务器密码机上，采用虚拟化技术创建出来的提供类同实体密码机服务的密码服务实例。

3.3

CHSM 数据影像 CHSM data image

简称 CHSM 影像。

包含 CHSM 内所有 VSM 中的与用户相关的配置、密钥及敏感信息等，并使用加密和签名机制保护影像的安全性。

用于 CHSM 的漂移过程。

3.4

VSM 数据影像 VSM data image

简称 VSM 影像。

包含 VSM 内与用户相关的配置、密钥及敏感信息等，并使用加密和签名机制保护影像的安全性。

用于 VSM 的漂移过程。

3.5

VSM 漂移 VSM drift

当一台 VSM 发生故障时，云平台管理系统自动将此 VSM 的数据影像导入至另外一台空闲正常的