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

主机内的密码运算资源和密钥存储资源。

3.4

单根 IO 虚拟化　single root I/O virtualization;SRIOV

使单根端口下的单个 PCIE 物理设备可针对管理程序或客户机操作系统显示为多个单独的虚拟 PCIE 设备(VF)的一种规范。

3.5

私钥访问控制码　private key access password

用于验证私钥使用权限的口令字。

3.6

虚拟密码机　virtual security module;VSM

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。

3.7

虚拟密码机数据影像　VSM data image

包含虚拟密码机内与用户相关的配置、密钥及敏感信息等。虚拟密码机数据影像的安全性使用加密和签名机制进行保护。

用于虚拟密码机的漂移过程。

3.8

虚拟密码机漂移　VSM drift

当一台虚拟密码机发生故障时,云平台管理系统自动将此虚拟密码机的数据影像导入至另外一台空闲正常的虚拟密码机上,并快速切换用户网络。在用户无感知的情况下,恢复虚拟密码机的可用性。

3.9

虚拟密码机镜像　VSM image

包含虚拟密码机所有软件(包括操作系统)及配置的模板文件。虚拟密码机镜像的安全性使用签名机制保护。

用于虚拟密码机的创建过程。

3.10

Web 服务　Web Service

一种应用编程接口或 Web 应用编程接口,通过标准的规约进行定义,并通过标准进行访问和使用。

4　缩略语

下列缩略语适用于本文件。

CBC:分组链接 (Cipher Block Chaining)

ECB:电子密本 (Electronic Codebook)

SRIOV:单根 IO 虚拟化(Single Root I/O Virtualization)

5　功能要求

5.1　设备形态

云服务器密码机在物理形态上表现为一台独立的密码设备,在逻辑上由一个宿主机和若干个虚拟密码机组成。云服务器密码机总体结构见图 1。

宿主机通过云服务器密码机管理接口接受云平台管理系统的管理和调度命令并执行,包括执行虚拟密码机的创建、启动、关闭、删除、漂移等操作。宿主机不提供密码服务。云服务器密码机的设备维护

通过宿主机进行。

云服务器密码机通过虚拟化技术实现多个虚拟密码机对物理设备的处理器、网络、存储等资源以及密码运算部件、密钥存储部件及随机数发生器等密码部件的共享与安全隔离。

虚拟密码机作为独立的密码服务单元为租户和应用提供密码服务，并对密码运算部件、密钥存储部件及随机数发生器进行调用。

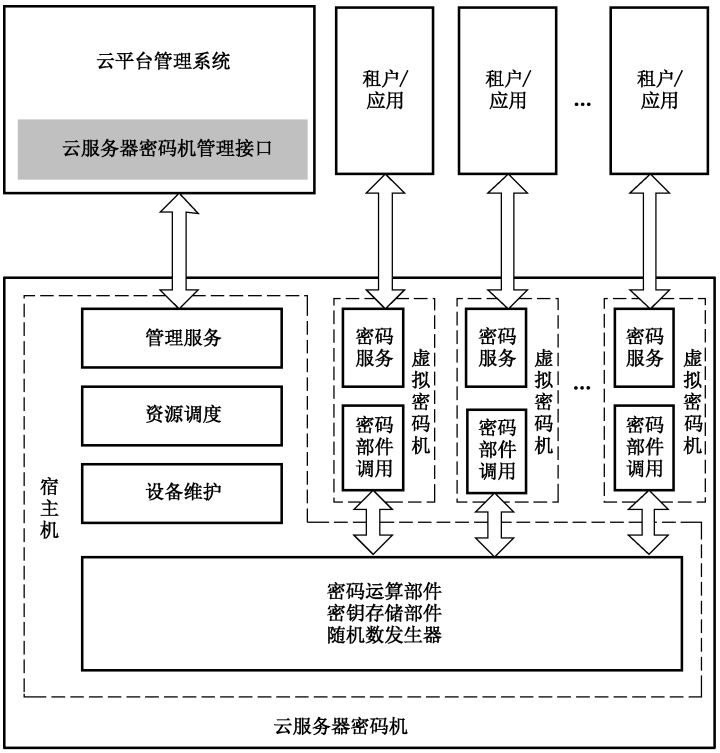

图 1　云服务器密码机总体结构

5.2　设备管理

5.2.1　管理要求

云服务器密码机的宿主机由云平台或云服务器密码机所有者进行管理和使用，虚拟密码机由租户管理和使用。

云服务器密码机宿主机和每个虚拟密码机应具备独立的管理界面和管理员，管理员通过管理界面进行密钥管理、配置以及日志审计等管理操作，不同的管理员应有不同的操作权限。管理员登录系统前应通过身份鉴别。宿主机和不同的虚拟密码机不能相互访问对方的管理员账号、口令文件和身份介质。

云服务器密码机的宿主机接受云平台管理系统的集中统一管理，管理接口和协议应符合 GM/T 0088 的要求。虚拟密码机不接受云平台管理系统的集中统一管理，可由虚拟密码机所属租户自己的管理系统进行集中统一管理。

云服务器密码机的宿主机和不同虚拟密码机的远程管理通道和维护通道应彼此独立，并采用加密和身份鉴别等技术手段对远程管理通道和维护通道进行保护。宿主机的管理员和维护人员不能登录虚拟密码机，不能获取虚拟密码机中的敏感信息，也不能访问虚拟密码机的服务。

宿主机的管理员具有对宿主机进行初始化和系统配置、密钥管理等操作权限，以及对虚拟密码机执

行创建、启动、关闭、删除、漂移等操作权限。宿主机的管理员不能对虚拟密码机执行初始化和系统配置、密钥管理等操作。虚拟密码机的管理员具有对所属虚拟密码机进行初始化和系统配置、密钥管理等操作权限，不能对宿主机和其他虚拟密码机执行初始化和系统配置、密钥管理等操作，也不能对虚拟密码机执行创建、启动、关闭、删除、漂移等操作。

5.2.2 初始化

云服务器密码机宿主机的初始化主要包括宿主机密钥的生成(恢复)与安装、生成管理员、按照安全机制对密钥进行安全存储和备份，使设备处于就绪状态。虚拟密码机的初始化主要包括虚拟密码机密钥的生成(恢复)与安装、生成管理员、生成或导入租户和虚拟密码机的数字证书或标识密码等身份鉴别信息，使虚拟密码机处于就绪状态。在正常使用虚拟密码机之前，需要完成租户和对应虚拟密码机身份鉴别信息的生成或导入。

5.2.3 注册、调度和监控

云服务器密码机宿主机宜具有向云平台管理系统进行注册的功能，登记本宿主机物理设备的物理资源(处理器、内存、网络、密码运算能力、密钥存储容量等)，同时接受云平台管理系统对其进行调度管理和运行状态的实时监控。

5.3 密码运算

虚拟密码机应具有对称密码运算、公钥密码运算以及密码杂凑运算等密码运算功能，并且支持多任务并发访问。

5.3.1 对称密码算法

虚拟密码机应至少支持 SM4 分组密码算法，至少包括电子密本(ECB)和分组密码链接(CBC)两种模式。

5.3.2 公钥密码算法

虚拟密码机应至少支持 SM2 公钥密码算法。

5.3.3 密码杂凑算法

虚拟密码机应至少支持 SM3 密码杂凑算法。

5.4 日志审计

云服务器密码机宿主机和不同虚拟密码机应提供日志记录、查看和导出功能。

宿主机的日志内容包括：

a) 登录认证、系统配置等管理员操作行为；

b) 虚拟密码机的创建、启动、关闭、删除、漂移等操作或事件及其结果；

c) 接受云平台管理系统的相应管理命令及操作。

虚拟密码机的日志内容包括：

a) 管理员操作行为，包括登录认证、系统配置、密钥管理等操作；

b) 异常事件，包括认证失败、非法访问等异常事件的记录。

日志的存储和操作应满足以下要求：

——宿主机和不同虚拟密码机的日志记录应独立存储和操作；
——宿主机和不同虚拟密码机的日志记录仅能由宿主机和不同虚拟密码机自身的管理员访问；
——宜提供关键日志记录的完整性校验或其他防篡改功能；
——宿主机和不同虚拟密码机的管理员不能相互访问对方的日志记录。

5.5 设备自检

云服务器密码机的宿主机和虚拟密码机应具有启动时自检和接收自检指令时自检的功能，宜具有周期性自检的功能。

宿主机自检宜包括以下功能：

a) 硬件部件自检；
b) 密码部件自检；
c) 虚拟化功能自检；
d) 物理网络检查；
e) 所存储数据的完整性检查。

虚拟密码机的自检宜包括以下功能：

a) 密码算法正确性检查；
b) 随机数发生器检查；
c) 虚拟网络检查；
d) 所存储密钥和数据的完整性检查。

5.6 设备使用

租户使用虚拟密码机可按以下过程进行：

a) 租户向云平台申请虚拟密码机，获得批准后得到虚拟密码机的管理 IP 地址、管理域名和管理端口、密码服务 IP、密码服务域名和密码服务端口以及默认管理员登录口令。
b) 租户访问虚拟密码机的管理 IP 地址并以默认管理员口令登录虚拟密码机，进行虚拟密码机的初始化操作，包括租户和对应虚拟密码机身份鉴别信息的生成或导入。
c) 租户以管理员身份登录虚拟密码机，进行系统配置和密钥管理操作。
d) 租户和虚拟密码机建立安全通道，并通过安全通道调用虚拟密码机的密码服务。对安全通道的相关要求见 9.1。

5.7 虚拟化

5.7.1 虚拟密码机生命周期管理

云服务器密码机应具备虚拟化功能，能接受外部命令，创建、启动、停止、销毁虚拟密码机。

5.7.2 虚拟密码机之间的密钥隔离

云服务器密码机应具备密钥隔离功能，防止虚拟密码机的密钥被盗用、防止虚拟密码机之间交叉使用密钥、防止宿主机管理员获取虚拟密码机密钥。

5.7.3 虚拟密码机镜像安全

虚拟密码机的镜像文件应进行签名保护，云服务器密码机应禁止签名验证不通过的虚拟密码机镜

像在云服务器密码机中运行。

5.7.4 虚拟密码机安全漂移

云服务器密码机宜支持虚拟密码机漂移功能。漂移过程中，虚拟密码机的数据影像应进行加密和完整性保护。

5.7.5 虚拟密码机资源调整

云服务器密码机宜支持虚拟密码机所占用资源（处理器、内存、网络、密码运算、密钥存储等）的调整功能。

5.7.6 虚拟密码机最大数量

云服务器密码机应定义并向云平台管理系统上报最大支持的虚拟密码机数量。

5.7.7 虚拟机密码机管理

虚拟密码机宜满足 GB/T 35293 提出的虚拟机管理通用要求。

6 安全要求

6.1 密钥管理

6.1.1 密钥管理功能

云服务器密码机的宿主机应具有宿主机所有密钥的产生、安装、存储、使用、销毁以及备份和恢复等功能，云服务器密码机的虚拟密码机应具有本虚拟密码机所有密钥的产生、安装、存储、使用、销毁以及备份和恢复等功能。宿主机不能管理和访问虚拟密码机的密钥，虚拟密码机不能管理和访问自身以外的其他虚拟密码机和宿主机的密钥。

6.1.2 密钥结构

云服务器密码机应至少支持三层密钥结构：管理密钥、用户密钥/设备密钥/密钥加密密钥、会话密钥。密钥结构见图 2。

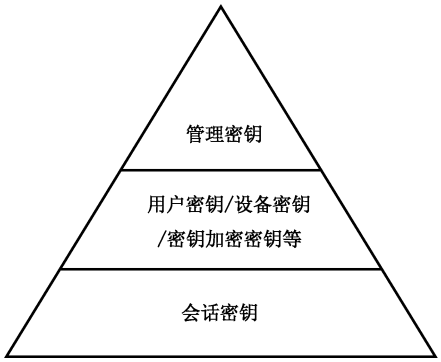

图 2 云服务器密码机密钥结构

管理密钥：用于保护其他密钥和敏感信息的安全，包括对其他密钥的管理、备份、恢复以及管理员身

份鉴别等。云服务器密码机的宿主机和各个虚拟密码机都具有自己的管理密钥。管理密钥应安全存储。

用户密钥：包括签名密钥对和加密密钥对，用于实现用户签名、验证、身份鉴别以及会话密钥的保护和协商等，代表租户或应用的身份。云服务器密码机的宿主机不使用和管理用户密钥，各个虚拟密码机采用各自的管理密钥加密存储各自的用户密钥，不同虚拟密码机不能相互访问用户密钥。

设备密钥：是云服务器密码机的身份密钥，包括签名密钥对和加密密钥对，用于设备管理，代表云服务器密码机的身份。云服务器密码机的宿主机和各个虚拟密码机都具有自己的设备密钥并采用各自的管理密钥加密存储。

密钥加密密钥：是定期更换的对称密钥，在预分配或导入导出密钥的情况下，虚拟密码机采用密钥加密密钥对会话密钥进行保护。

会话密钥：用于数据加解密。

6.1.3 密钥产生及安装

管理密钥：由设备初始化时使用的管理工具生成或者安装，存储在云服务器密码机内部的安全存储区域。云服务器密码机的宿主机和各个虚拟密码机应使用各自独立的管理工具产生各自的管理密钥并存储在各自独立的安全存储区域。

用户密钥：云服务器密码机的虚拟密码机各自的用户签名密钥对由虚拟密码机各自产生和安装，应使用物理噪声源产生的随机数和强素数生成用户签名密钥对；用户加密密钥对由密钥管理系统生成并独立分发到各个虚拟密码机，加密密钥对分发的格式应遵循 GB/T 36322 对加密密钥对保护格式的要求。

设备密钥：云服务器密码机的宿主机和各个虚拟密码机应使用各自独立的管理工具产生各自的设备签名密钥对，应使用物理噪声源产生的随机数和强素数生成设备签名密钥对，设备加密密钥对由密钥管理系统生成并独立分发到宿主机和各个虚拟密码机，设备加密密钥对分发的格式应遵循GB/T 36322对加密密钥对保护格式的要求。

密钥加密密钥：云服务器密码机的虚拟密码机应使用各自独立的管理工具产生各自的密钥加密密钥并对会话密钥进行加密保护，应使用物理噪声源产生的随机数生成密钥加密密钥。

会话密钥：应使用物理噪声源产生的随机数生成会话密钥，应支持一次会话更换一次会话密钥。

6.1.4 密钥安全存储和销毁

云服务器密码机的每个虚拟密码机应能够至少保存 32 对非对称密钥和 100 个对称密钥。

云服务器密码机应对持久性保存的密钥安全存储，并符合 GB/T 37092 安全二级及以上对敏感安全参数管理的规定。

虚拟密码机的设备密钥、用户密钥和密钥加密密钥采用该虚拟密码机的管理密钥加密存储在各虚拟密码机独立的安全存储区域，各虚拟密码机均应支持一定数量的密钥存储，会话密钥长期存储时应使用用户密钥对或密钥加密密钥进行加密保护。

虚拟密码机管理密钥的安全存储宜采用租户授权模式，避免宿主机和其他虚拟密码机/租户的访问，可采用以下方式：

——采用授权码结合其他密钥分量作为密钥素材加密存储，其他密钥分量可采用随机数和硬件特征码（如以太网卡的 MAC 地址、硬盘序列号等）等信息；

——在具有微电保护和毁钥触发装置的密钥存储部件上存储并采用授权码进行访问控制；

——在智能密码钥匙等外置密码模块上存储并采用授权码进行访问控制。

不同的虚拟密码机应具有不同的授权码，授权码由租户保管和使用，虚拟密码机的管理员口令或智能密码钥匙的 PIN 码可以作为授权码使用。

宿主机的设备密钥采用宿主机的管理密钥加密存储。宿主机的管理密钥需加密存储或者采用具有微电保护和毁钥触发装置的密钥存储部件进行安全存储，虚拟密码机和租户不能访问宿主机的管理密钥。

宿主机和虚拟密码机应各自具备独立的密钥销毁功能。执行密钥销毁时，宿主机和虚拟密码机各自存储的指定密钥应按照 GB/T 37092 安全二级及以上的要求进行置零操作。具有微电保护的密钥存储部件在毁钥触发装置被触发时对所存储的所有密钥进行置零操作。

6.1.5 密钥使用

云服务器密码机在密钥使用方面，应符合 GB/T 37092 安全二级及以上对敏感安全参数管理的规定，并满足以下要求：

a) 设备密钥的使用不对租户和应用开放；

b) 除公钥外，所有密钥均不能以明文形式出现在云服务器密码机外；虚拟密码机公钥以外的所有密钥均不能以明文形式出现在虚拟密码机运行空间和安全存储区之外；

c) 云服务器密码机应具备防止非法使用和导出密钥的权限控制机制。宿主机不能导出和使用虚拟密码机的密钥，虚拟密码机不能导出和使用其他虚拟密码机的密钥，租户只能导出和使用所属虚拟密码机的密钥。应为不同的虚拟密码机采用不同的私钥访问控制码进行私钥使用的控制。

6.1.6 备份/恢复

对持久性保存的密钥，云服务器密码机应具备备份/恢复功能。

备份操作产生的备份文件应以密文形式存储到云服务器密码机外的存储介质中，加密备份文件的密钥应有安全机制保证其安全。

备份出的密钥可以恢复到云服务器密码机中，同厂家的不同型号的云服务器密码机之间应能够互相备份恢复。宿主机的密钥恢复操作只能在宿主机中进行，虚拟密码机的密钥恢复操作只能在虚拟密码机中进行。

6.2 访问控制与身份鉴别

云服务器密码机应具备身份鉴别机制。宿主机和管理员之间、虚拟密码机和管理员之间、使用虚拟密码机的租户/应用和虚拟密码机之间应进行身份的双向鉴别，并符合 GB/T 37092 安全二级及以上对管理员和用户的身份鉴别的规定，宜采用基于数字证书、标识密码或硬件身份介质的身份鉴别机制。

登录宿主机或虚拟密码机应具备完善的身份鉴别机制，不同的管理操作应有不同的操作权限。宿主机或虚拟密码机应拒绝任何不具备相应权限的访问或操作，防止未经授权的恶意人员登录，以避免破坏宿主机和虚拟密码机的安全性。

云服务器密码机应能够为内部存储的数据和资源提供访问控制功能：

——对于存储在虚拟密码机内部的私钥，应持有正确的私钥访问控制码才能使用；

——对虚拟密码机服务接口的调用和对宿主机和虚拟密码机的远程管理，可采用基于 IP 地址的授权访问控制技术，只有具备已授权 IP 地址的主机才可正常调用虚拟密码机服务接口或对宿主机和虚拟密码机进行远程管理，不具备授权 IP 的主机不准许调用虚拟密码机服务接口或对宿

主机和虚拟密码机进行远程管理；

——对不同虚拟密码机的访问应由所访问虚拟密码机的管理员单独授权。

6.3 随机数生成和检验

每个虚拟密码机应具备独立的随机数生成功能，虚拟密码机生成的随机数应符合 GB/T 32915 的要求以及 GM/T 0062 对 E 类产品的规定。虚拟密码机之间共享物理噪声源时，应通过虚拟化技术进行逻辑隔离，应确保不同的随机数提供给不同的虚拟密码机使用，并对已使用的随机数执行置零操作。

6.4 硬件安全

云服务器密码机的硬件应符合 GB/T 37092 安全二级及以上对硬件模块物理安全的规定。

云服务器密码机应提供安全措施，保证密码算法、密钥、关键数据的存储安全。

除必需的通信接口和管理接口以外，不提供任何可供调试、跟踪的外部接口。内部的调试、检测接口应在产品定型后封闭。

云服务器密码机应防止通过非授权的任何外部接口获得云服务器密码机或虚拟密码机中的敏感信息。

云服务器密码机在工艺设计、结构设计、硬件配置等方面要采取相应的保护措施，保证设备基本的物理安全防护功能。

6.5 软件安全

云服务器密码机的软件和固件应符合 GB/T 37092 安全二级及以上对软件/固件安全的规定。

所有的安全协议及管理软件应自主实现。

操作系统应进行安全加固，裁减一切不需要的功能，关闭所有不需要的端口和服务。

任何操作指令及其任意组合，不能泄露密钥和敏感信息。

云服务器密码机只接受合法的操作指令。

6.6 虚拟机安全

虚拟密码机应满足 GB/T 35293 提出的虚拟机安全性管理要求以及 GB/T 31168 提出的系统虚拟化、网络虚拟化和存储虚拟化安全性要求。

6.7 安全隔离

6.7.1 管理隔离

宿主机和不同的虚拟密码机应具备不同的管理 IP 地址、管理域名或管理端口，运行不同的管理进程，并采用不同的安全通道进行远程管理或远程维护。

同一个终端设备不能同时登录宿主机和不同的虚拟密码机。

宿主机和不同的虚拟密码机之间不能共享用户信息，应进行完全独立的用户管理。

宿主机和不同的虚拟密码机应具备独立的管理界面和管理员。

6.7.2 使用隔离

不同的虚拟密码机应采用不同的服务 IP 地址、服务域名或服务端口并采用不同的安全通道对外提供密码服务。

宿主机和不同的虚拟密码机应通过不同的进程访问密码运算部件、密钥存储部件、随机数发生器等密码部件，并具备不同的识别标识，用于密码部件或驱动程序对来自宿主机和不同虚拟密码机的访问请求进行区分。

当采用软件或固件模块提供密码运算时，宿主机和不同的虚拟密码机应采用不同的 CPU 物理核实现密码运算。

6.7.3 系统隔离

虚拟密码机应实现 CPU 上下文、内存、持久性存储、网络协议栈、文件系统、进程管理、用户管理等系统要素的独立运行和相互隔离：

——虚拟密码机宜占用独立的 CPU 处理核。共享 CPU 处理核的虚拟密码机宜属于同一个租户。可通过 CPU 亲和性的设置进行虚拟密码机和 CPU 处理核的绑定。

——运行中的虚拟密码机宜使用专属内存，不宜使用 swap 等内存交换技术，可采用内存限额和保留内存的方式避免不同虚拟密码机的内存共享。

——虚拟密码机的持久性存储区域可采用加密文件系统和文件/目录访问控制等技术进行安全隔离保护。不同虚拟密码机的持久性存储加密保护应采用不同的密钥，宿主机和不同的虚拟密码机应采用不同的目录或文件进行持久性存储，同一虚拟密码机的持久性存储文件/目录不能由不同的租户/用户共享。

——虚拟密码机应具备独立运行的网络协议栈、文件系统、进程空间和用户空间。可采用为不同的虚拟密码机运行不同的客户操作系统(GuestOS)或命名空间(Namespace)的方式实现网络协议栈、文件系统、进程空间和用户空间等系统资源的封装和隔离。

6.7.4 密钥隔离

宿主机和不同虚拟密码机应具有各自完全独立的管理密钥、设备密钥、用户密钥、密钥加密密钥和会话密钥，密钥结构应按照 6.1.2 的要求，完全独立产生，层层加密保护。

最顶层的管理密钥应按照 6.1.4 的要求进行存储，宿主机和不同虚拟密码机的管理密钥采用不同的授权码进行访问控制。宿主机的授权码由宿主机管理员保管，不同虚拟密码机的授权码由各自租户保管和使用。

6.7.5 密码部件隔离

可采用基于硬件或软件的虚拟化技术对云服务器密码机的密码部件在虚拟密码机之间进行安全隔离与共享。

——密码运算部件、密钥存储部件、随机数发生器等密码部件内部，可采用物理或逻辑的方式，为宿主机和不同的虚拟密码机划分不同的运算单元和存储空间。

——密码部件的 IO(输入输出)接口可采用硬件虚拟化(如 SRIOV)或在驱动程序和 API 层进行访问控制等物理或逻辑的方式为宿主机和不同的虚拟密码机划分不同的数据和控制命令传输通道。

——当采用 SRIOV 等硬件虚拟化技术进行密码部件的共享时，应为不同的虚拟密码机分配独立的虚拟密码部件(VF)。应采用技术手段防止虚拟密码机访问未分配给自己的虚拟密码部件(VF)。在硬件和底层操作系统支持虚拟设备视图的情况下，可为不同的虚拟密码机创建独立的设备视图，该视图仅包含分配给本虚拟密码机的虚拟密码部件设备(VF)。在硬件和底层操作系统不支持虚拟设备视图的情况下，可统一对虚拟密码部件进行命名，并将虚拟密码机的密

码部件设备驱动程序和分配给本虚拟密码机的命名虚拟密码部件绑定，命名参数在虚拟密码初始化时传入，设备驱动程序内部仅允许对匹配命名参数的虚拟密码机进行访问。

——当不采用 SRIOV 等硬件虚拟化技术进行密码部件的共享时，不同的虚拟密码机应通过统一的设备驱动程序或 API 中间层对密码部件进行调用。可通过为不同的虚拟密码机分配不同的设备句柄或任务 ID 进行虚拟密码机的区分和隔离。

6.7.6 网络隔离

可采用基于硬件或软件的虚拟化技术对云服务器密码机的网络接口在虚拟密码机之间进行安全隔离与共享。

——当采用 SRIOV 等硬件虚拟化技术进行网络接口的共享时，应为不同的虚拟密码机分配独立的虚拟网络接口(VF)，并为虚拟网络接口分配不同的 MAC 地址。可结合 VLAN 和 VXLAN 等网络隔离技术进一步实现虚拟网络接口广播域的隔离。

——当不采用 SRIOV 等硬件虚拟化技术进行网络接口的共享时，可通过软件实现的虚拟交换机进行不同虚拟密码机的网络隔离。为虚拟交换机配置虚拟网络接口并接入虚拟交换机，物理网络接口也接入虚拟交换机，不同的虚拟网络接口应具有不同的 MAC 地址。可结合 VLAN 和 VXLAN 等网络隔离技术进一步实现广播域的隔离。

6.8 安全漂移

虚拟密码机可在共享密钥的云服务器密码机之间进行虚拟机漂移，采用共享密钥对需要漂移的虚拟密码机的数据影像进行加密和完整性保护。

云服务器密码机也可采用专用的非对称密钥对进行虚拟密码机的安全漂移。云服务器密码机各自拥有用于虚拟密码安全漂移的专用非对称密钥对，并对公钥进行发布和共享。作为漂移源端的云服务器密码机采用目的端云服务器密码机发布的公钥并结合数字信封技术，对需要漂移的虚拟密码机的数据影像进行加密，并采用自身的私钥对该数据影像进行数字签名以保护完整性。漂移目的端的云服务器密码机采用自身的私钥并结合数字信封技术对漂移来的虚拟密码机的数据影像进行解密，并采用源端云服务器密码机发布的公钥对该数据影像进行签名验证。

6.9 设备状态

云服务器密码机的虚拟密码机在设备状态方面，应满足以下要求：

a) 虚拟密码机应具有初始、就绪和关闭状态，宜具有挂起状态；

b) 已经创建并启动但未安装设备密钥的虚拟密码机应处于初始状态，已经启动并已安装设备密钥的虚拟密码机应处于就绪状态，收到停止命令的虚拟密码机应进入挂起状态，收到关闭命令的虚拟密码机应进入关闭状态；

c) 在初始状态下，除读取设备信息以及设备密钥的生成或恢复操作外，不能执行任何操作，生成或恢复设备密钥后，虚拟密码机处于就绪状态；

d) 在就绪状态下，除设备密钥的生成或恢复操作外，能执行任何操作；

e) 在就绪状态下进行的密钥管理操作，管理员应和虚拟密码机进行身份鉴别；

f) 在就绪状态下收到停止命令的虚拟密码机进入挂起状态，在挂起状态下，虚拟密码机不提供密码服务，虚拟密码机管理员不能进行任何操作，虚拟密码机的运行时状态信息以及关键和敏感安全参数备份后加密存储，在挂起状态下收到启动命令的虚拟密码机在解密并恢复运行时状态信息以及关键和敏感安全参数后重新进入就绪状态；

g) 收到关闭命令的虚拟密码机应进入关闭状态，虚拟密码机关闭过程中应关闭密码服务和对外接口，将关键和敏感安全参数置零，释放所占用的 CPU、内存、IO 接口、持久化存储和密码部件等资源；

云服务器密码机的宿主机在设备状态方面，应满足以下要求：

a) 宿主机应具有初始和就绪两个状态；

b) 未安装设备密钥的宿主机应处于初始状态，已安装设备密钥的宿主机应处于就绪状态；

c) 在初始状态下，除读取设备信息以及设备密钥的生成或恢复操作外，不能执行任何操作，生成或恢复设备密钥后，宿主机处于就绪状态；

d) 在就绪状态下，除设备密钥的生成或恢复操作外，能执行任何操作；

e) 在就绪状态下进行的密钥管理操作，管理员应和宿主机进行身份鉴别。

7 硬件要求

7.1 对外接口

云服务器密码机应分别提供服务接口和管理接口，可以通过物理或虚拟网络与服务对象和管理平台连接。云服务器密码机应支持 RJ-45 或光纤等物理硬件接口，支持以太网和 TCP/IP 网络通信协议。虚拟密码机共享云服务器密码机的物理硬件接口，并通过虚拟化技术进行逻辑隔离。

7.2 随机数发生器

云服务器密码机应提供多路随机源，并至少采用两个独立的物理噪声源芯片实现。虚拟密码机的随机数应来自于至少两个独立的物理噪声源芯片。物理噪声源芯片或提供物理噪声源的密码模块应通过商用密码认证。云服务器密码机提供的物理噪声源应能从整体性能上满足所支持的最大数量虚拟密码机的随机数产生需求。

7.3 环境适应性

云服务器密码机的工作环境应符合 GB/T 9813.3 中关于“气候环境适应性”的规定。

7.4 可靠性

云服务器密码机的平均无故障工作时间应不低于 10 000 h。虚拟密码机的故障和切换应不影响云服务器密码机的整体可靠性。

8 软件要求

8.1 基本要求

云服务器密码机底层软件应采用模块化设计，应通过技术措施防止用户的非法调用。宿主机和虚拟密码机运行的软件之间不能够相互调用，不同虚拟密码机运行的软件之间也不能够相互调用。

8.2 管理工具

云服务器密码机的宿主机及不同虚拟密码机宜具备独立的管理工具。

9 接口规范

9.1 服务接口

虚拟密码机可采用 API 或者 Web 服务接口对外提供密码服务。

API 应符合 GB/T 36322 的规定。API 采用本地调用方式，可由 C、PYTHON、JAVA 等开发语言实现。API 和虚拟密码机之间的通信报文格式可自定义。

Web 服务接口可采用 JSON 或 XML 等主流的 Content Type（内容类型）编码，宜具备和 GB/T 36322 的兼容性。采用 HTTP JSON 编码的 Web 服务接口消息语法见附录 A。

应建立安全通道，对密码服务调用过程进行身份鉴别以及消息的机密性和完整性保护。可采用传输层密码协议（TLCP）、IPSec 协议或自定义密码协议建立安全通道：

——如果采用传输层密码协议（TLCP），应采用 GB/T 38636 中定义的协议；

——如果采用 IPSec 协议，应采用 GB/T 36968 中定义的协议；

——如果采用自定义密码协议，应符合密码国家标准、行业标准的相关要求。

9.2 管理接口

云服务器密码机的管理接口和协议应符合 GM/T 0088 的规定，管理服务运行在宿主机上，接受云平台管理系统的管理和调度命令并执行，包括执行虚拟密码机的创建、启动、关闭、删除、漂移等操作。

虚拟密码机宜提供各种密码运算服务、密钥管理服务的注册、发布、发现、获取和编排接口。

10 检测要求

10.1 检测说明

检测要求规定了云服务器密码机的通用检测内容和方法。检测应包括外观和结构检查、提交文档的检查、功能检测、性能检测和环境适应性检测等。

10.2 外观和结构的检查

根据产品的物理参数，对云服务器密码机的外观、尺寸、内部部件及附件进行检查。

10.3 提交文档的检查

云服务器密码机研制单位按照商用密码认证机构的检测要求提交相关文档资料，作为云服务器密码机的检测依据。

10.4 功能检测

10.4.1 检测说明

云服务器密码机的功能检测目的是测试云服务器密码机各项功能的运行情况，并检验功能实现的正确性。

10.4.2 初始化检测

在云服务器密码机正常启动后，对云服务器密码机进行初始化功能检测。初始化检测主要包括宿

主机和虚拟密码机的配置、生成管理员、密钥的生成(恢复)与安装,使宿主机和虚拟密码机处于正常工作状态。云服务器密码机应能够正常初始化,检测结果符合 5.2.2 的要求。

10.4.3 密码运算检测

云服务器密码机的密码运算检测方法是将虚拟密码机的密码运算结果与已知的正确结果进行比较,如果计算结果和正确结果相同,则测试通过;否则,测试失败。

密码运算检测的范围应包括虚拟密码机提供的每个对称密码算法、非对称密码算法和杂凑算法的每个功能函数,如:加密、解密、杂凑、数字签名、验证签名等,其中对称密码算法的检测应测试虚拟密码机支持的各种工作模式。对云服务器密码机进行密码运算检测的检测结果应符合 5.3 的要求。

10.4.4 密钥管理检测

云服务器密码机的密钥管理检测范围包括宿主机和虚拟密码机各种密钥的产生、安装、存储、使用、销毁以及备份和恢复等操作,通过使用云服务器密码机的管理工具进行测试。对云服务器密码机进行密钥管理检测的检测结果应符合 6.1 的要求。

10.4.5 随机数检测

按照 GM/T 0062 中 E 类产品的要求对云服务器密码机进行随机数检测,宿主机应能通过送样检测、出厂检测、上电检测和使用检测,虚拟密码机应能通过使用检测。

10.4.6 设备管理检测

设备管理检测包括管理操作检测、管理登录检测、管理接口检测、日志审计检测。

——管理操作检测,通过使用宿主机和虚拟密码机的管理工具或管理界面,对宿主机和虚拟密码机的不同管理操作设置不同的操作权限,并进行宿主机和虚拟密码机的配置、管理员的添加和删除、密钥的生成和管理等操作。

——管理登录检测,管理员登录宿主机或虚拟密码机前应通过身份鉴别,任何未通过身份鉴别或不具备相应权限的访问或操作都应被拒绝,检测结果应符合 5.2.1 的要求;宿主机和不同虚拟密码机的管理员不能相互访问对方的管理员账号、口令文件和身份介质。

——管理接口检测,通过云平台管理系统对云服务器密码机进行 GM/T 0088 中各项管理功能的检测,检测结果应符合 5.2.1 的要求。

——日志审计检测,通过使用宿主机和虚拟密码机的日志管理工具或界面进行宿主机和虚拟密码机的日志审计检测。对云服务器密码机进行日志审计检测的检测结果应符合 5.4 的要求。

10.4.7 设备自检检测

对云服务器密码机的宿主机和虚拟密码机分别进行启动时自检和接收自检指令时自检检测,检测结果应符合 5.5 的要求。

10.4.8 服务接口检测

虚拟密码机对外提供带有客户端的 API 时,应按照 GB/T 36322 的要求,对虚拟密码机进行应用编程接口检测:

——对于正确的调用环境和调用过程,API 函数应该返回正确的结果,并完成相应功能;

——对于设定的不正确的调用环境和调用过程,API 函数应返回相应的错误代码。

虚拟密码机对外提供无客户端的 Web 服务接口时，虚拟密码机的消息报文格式可遵循附录 A，也可按照 GB/T 36322 的要求设计相应的 HTTP 消息报文，对云服务器密码机进行请求-响应的消息报文检测：

——对于正确的请求消息报文，虚拟密码机应该返回正确的响应消息报文，并完成相应功能；

——对于设定的不正确的请求消息报文，虚拟密码机返回的响应消息报文应带有相应的错误代码。

10.4.9 管理工具检测

分别使用宿主机和虚拟密码机的管理工具或管理界面进行云服务器密码机的管理工具检测，检测结果应符合 8.2 的要求。

10.4.10 虚拟密码机检测

通过宿主机管理工具或云平台管理系统对云服务器密码机进行虚拟密码机的创建、启动、关闭、删除、漂移、镜像加载、资源调整等管理操作，并测试宿主机和各虚拟密码机之间能否相互访问，检测结果应符合 5.6 的要求。

10.4.11 安全性检测

虚拟密码机安全性测试按照 GM/T 0039 对固件模块或混合固件模块安全二级及以上的要求进行。

10.5 性能检测

10.5.1 检测说明

目的是测试云服务器密码机的系统容量以及进行各项密码运算的速度指标。

下列各项速度性能测试中的测试量由数据报文长度和测试次数决定。可以根据各个测试项的具体耗时情况，依照等比序列来选取测试次数，例如：测试次数 N 可以选择 1 次、10 次、100 次、1 000 次等，分别测试后得到不同测试次数时的性能序列。数据报文长度的选择在各个速度性能测试项中分别定义。

在 10.5.3、10.5.6 和 10.5.7 中包含的各个测试项的速度性能的计算如式(1)所示：

$$S=8LN/(1\ 024*1\ 024T) \quad \cdots\cdots(1)$$

式中：

S ——速度，单位为兆比特/秒(Mb/s)；

L ——数据报文的长度，单位为字节；

N——测试次数；

T ——测量所耗费的时间，单位为秒(s)。

在 10.5.4、10.5.5 和 10.5.8 中包含的各个测试项的速度性能的计算如式(2)所示：

$$S=N/T \quad \cdots\cdots(2)$$

式中：

S ——速度，单位为次每秒(次/s)；

N——测试次数；

T ——测量所耗费的时间，单位为秒(s)。

以下 10.5.3～10.5.8 的各项性能测试，均包括两种情况：单一负载和满负载。单一负载指云服务器

密码机仅启动一个虚拟密码机并将所有计算资源分配给该虚拟密码机时，该虚拟密码机的各项性能测试数据；满负载指按照 10.5.2 的测试结果创建和启动该云服务器密码机支持的最大数量虚拟密码机并对所有虚拟密码机并行进行各项性能测试时，所有虚拟密码机的各项性能测试数据之和、平均数据、最大及最小数据。

10.5.2 虚拟密码机最大数量测试

通过宿主机管理工具或云平台管理系统对云服务器密码机连续进行虚拟密码机的创建和启动操作，每个虚拟密码机的资源分配按照厂家指定的最低资源配额进行，直至无法创建和启动新的虚拟密码机，此时能够正常提供密码运算服务的虚拟密码机数量即为该云服务器密码机支持的最大虚拟密码机数量。

10.5.3 对称密码算法的加解密性能测试

将一个定长数据报文(建议为 1 024 字节)，发送给虚拟密码机进行对称密码算法加/解密操作，重复操作 N 次，测量其完成时间 T。用于测试的数据由检测机构选取，测试应进行三次以上，结果取平均值。

如虚拟密码机支持多种对称算法，应测试所支持的所有对称密码算法及其各种工作模式和使用方式(如加密、解密、MAC 等)。

对称密码算法的加解密性能单位统一为兆比特/秒(Mb/s)。

10.5.4 非对称密码算法的加解密性能测试

将一个定长数据报文(建议为 1 024 字节)，发送给虚拟密码机进行非对称密码算法加/解密操作，重复操作 N 次，测量其完成时间 T。用于测试的数据由检测机构选取。测试应进行三次以上，结果取平均值。

如虚拟密码机支持多种非对称算法，应测试所支持的所有非对称密码算法及其各种应用模式。

非对称密码算法的加解密性能单位统一为次/秒(tps)。

10.5.5 非对称密码算法的签名验签性能测试

将一个定长数据报文(建议为 1 024 字节)的杂凑值，发送给虚拟密码机进行签名/验签操作，重复操作 N 次，测量其完成时间 T。用于测试的数据由检测机构选取。测试应进行三次以上，结果取平均值。

如虚拟密码机支持多种非对称算法，应测试所支持的所有非对称密码算法及其各种应用模式。

非对称密码算法的签名/验签性能单位统一为次/秒(tps)。

10.5.6 密码杂凑算法性能测试

将一个定长数据报文，发送给虚拟密码机进行密码杂凑运算，重复操作 N 次，测量其完成时间 T。用于测试的数据由检测机构选取。测试应进行三次以上，结果取平均值。

密码杂凑算法性能单位统一为兆比特/秒(Mb/s)。

10.5.7 随机数发生器性能测试

让虚拟密码机生成并输出长度为 L 的符合随机特性的随机序列 N 组，测量其完成时间 T。测试应进行三次以上，结果取平均值。

随机数发生器性能单位统一为兆比特/秒(Mb/s)。

10.5.8 非对称密钥生成性能测试

让虚拟密码机生成并输出指定数量的密钥对,测量其完成时间 T。测试应进行三次以上,结果取平均值。

非对称密钥生成性能单位统一为对/秒(tps)。

10.6 环境适应性检测

环境适应性检测应按照 GB/T 9813.3—2017 中“5.8 环境试验”的要求进行,其结果应符合该标准中“4.8 环境条件”的要求。

11 合格判定

10.4 的各项检测中,其任意一项检测结果不合格,判定为产品不合格。

附 录 A
（资料性）
云服务器密码机 Web 服务接口消息语法

A.1 概述

本附录将对 GB/T 36322—2018 中 API 的调用和返回转换为在 WEB 应用和 HTTP 协议中使用的请求和响应，API 函数接口的输入参数在 HTTP 请求消息中编码传递，API 函数接口的输出参数及返回值在 HTTP 响应消息中编码。

本附录只描述了从函数接口到对应 HTTP 格式的转换规则，而不再具体描述 GB/T 36322 的每个函数到 HTTP 请求响应消息的转换过程。

A.2 函数接口数据类型到 HTTP 格式的转化规则

函数接口数据类型到对应 HTTP 格式的转换规则见表 A.1。

表 A.1 函数接口数据类型到 HTTP 格式的转化规则

C 语言类型	JSON 数据类型	备注
整型(unsigned int/int)	string	16 进制密钥索引、算法标识、函数返回代码、长度等数字的文本形式，如索引 1 被表示为“0x00000001”，算法标识 0x00000101 被表示为“0x00000101”，函数返回代码 0x01000001 被表示为“0x01000001”
句柄(void *)	string	16 进制句柄数值(一般为指针类型的地址)的文本形式
字符/字节串(unsigned char *)	string	16 进制字符/字节串的文本形式
结构体(struct)	Object	设备信息、公私钥结构、ECC 签名/加密结构等

A.3 函数调用与 HTTP 请求的转换规则

函数调用在转换为 HTTP 时，被转化为 HTTP Request body 中以 Json 格式表示的数据，原则如下：

a) 所有请求都采用 HTTP 的 POST 模式；

b) 函数名被作为 URL 的路径。

以 GB/T 36322—2018 中 6.4.8 外部密钥 ECC 公钥加密函数调用为例，其转换后 HTTP 请求如下：

```
POST /SDF_ExternalEncrypt_ECC HTTP/1.1\r\n
Content-Type: application/json \r\n
Content-Length: 实际请求 body 长度\r\n
\r\n
{
    “version”:“v1”,
```

```
    "reqType":"SDF_ExternalEncrypt_ECC",
    "request":{
        "hSessionHandle":"十六进制任务句柄数值的文本形式",
        "uiAlgID":"十六进制算法标识的文本形式",
        "ECCrefPublicKey":{
            "bits":"十六进制密钥位长的文本形式",
            "x":"十六进制公钥 x 坐标的文本形式",
            "y":"十六进制公钥 y 坐标的文本形式"
        },
        "pucData":"十六进制待加密数据明文的文本形式",
        "uiDataLength":"十六进制待加密数据明文长度的文本形式"
    }
}
```

注 1：Content-Type 和 Content-Length 是 HTTP 协议的标准字段，此处按照其原意进行使用。

注 2：对应 HTTP 协议中的其他标准字段如 Host，User-Agent 等，与本章节无关，在此不再标出。

A.4 函数响应与 HTTP 响应的转换规则

函数调用返回在转换为 HTTP 时，被转化为 HTTP Response body 中以 Json 格式表示的数据，以 GB/T 36322—2018 中 6.4.8 外部密钥 ECC 公钥加密函数调用返回为例，其转换后 HTTP 响应如下：

```
HTTP 200 OK\r\n
    Content-Type: application/json;charset=UTF-8\r\n
    Content-Length: 实际响应 body 的长度\r\n
    \r\n
    {
        "version":"v1",
        "reqType":" SDF_ExternalEncrypt_ECC",
        "response":{
            "result": 成功为 true,失败为 false
            "retcode":"十六进制函数调用返回值的文本形式"
            "ECCCipher":{
                "x":"十六进制 X 分量的文本形式",
                "y":"十六进制 y 分量的文本形式",
                "M":"十六进制明文杂凑值的文本形式",
                "L":"十六进制密文长度的文本形式",
                "C":"十六进制密文的文本形式"
            }
        }
    }
```