



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	III
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 功能要求	2
5.1 设备形态	2
5.2 设备管理	3
5.3 密码运算	4
5.4 日志审计	4
5.5 设备自检	5
5.6 设备使用	5
5.7 虚拟化	5
6 安全要求	6
6.1 密钥管理	6
6.2 访问控制与身份鉴别	8
6.3 随机数生成和检验	9
6.4 硬件安全	9
6.5 软件安全	9
6.6 虚拟机安全	9
6.7 安全隔离	9
6.8 安全漂移	11
6.9 设备状态	11
7 硬件要求	12
7.1 对外接口	12
7.2 随机数发生器	12
7.3 环境适应性	12
7.4 可靠性	12
8 软件要求	12
8.1 基本要求	12
8.2 管理工具	12
9 接口规范	13
9.1 服务接口	13
9.2 管理接口	13
10 检测要求	13

10.1 检测说明 13

10.2 外观和结构的检查 13

10.3 提交文档的检查 13

10.4 功能检测 13

10.5 性能检测 15

10.6 环境适应性检测 17

11 合格判定 17

附录 A（资料性） 云服务器密码机 Web 服务接口消息语法 18

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。

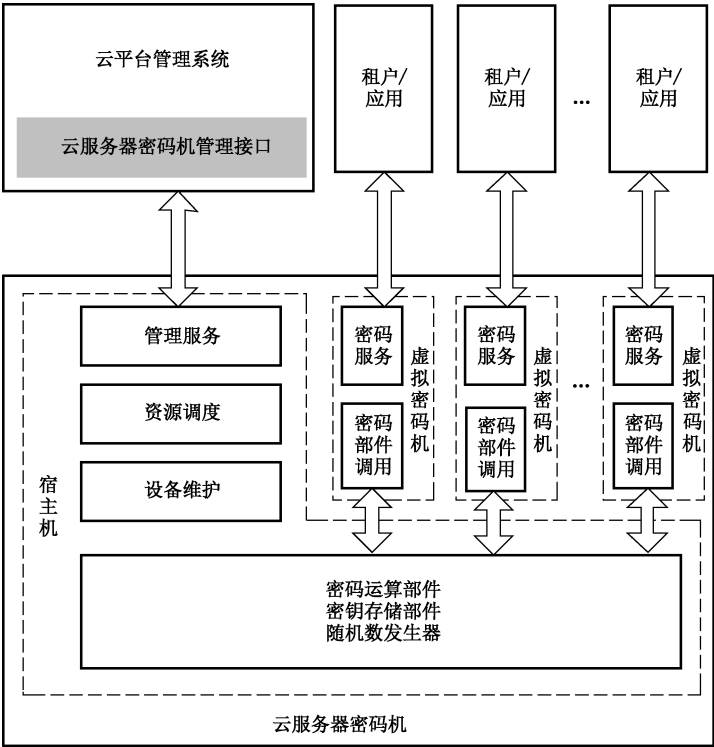


图 1 云服务器密码机总体结构

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。

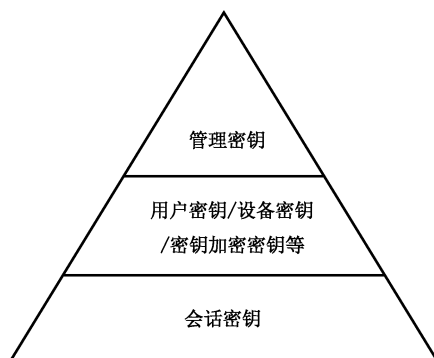


图 2 云服务器密码机密钥结构

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;

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/695142204311011243>