ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0142—2024

云服务器密码机检测规范

Cloud host cryptographic server test specification

2024-12-27 发布　　2025-07-01 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：商用密码检测认证中心、北京信安世纪科技有限公司、三未信安科技股份有限公司、兴唐通信科技有限公司、卫士通信息产业股份有限公司、北京江南天安科技有限公司、山东渔翁信息技术股份有限公司、北京数字认证股份有限公司、格尔软件股份有限公司、鼎铉商用密码测评技术（深圳）有限公司、智巡密码（上海）检测技术有限公司。

本文件主要起草人：李国友、陈妍、孙艺铭、汪宗斌、胡耀华、顾伟平、李冬、邓开勇、刘芳、雷银花、李小雨、燕爽、秦体红、张宇、高志权、刘会议、姚长远、何济尘、罗俊、李国、马晓艳、张钊、郭刚、吴震、赵松、王春涛、吴远成、郝波、李振、邹家须、包斯刚、韩玮。

云服务器密码机检测规范

1 范围

本文件规定了云服务器密码机的检测环境、检测内容、检测方法、送检技术文档要求和判定规则。

本文件适用于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 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 15852.2 信息技术 安全技术 消息鉴别码 第 2 部分：采用专用杂凑函数的机制

GM/T 0005 随机性检测规范

GM/T 0018 密码设备应用接口规范

GM/T 0022 IPSec VPN 技术规范

GM/T 0024 SSL VPN 技术规范

GM/T 0028 密码模块安全技术要求

GM/T 0039 密码模块安全检测要求

GM/T 0062 密码产品随机数检测要求

GM/T 0088 云服务器密码机管理接口规范

GM/T 0104—2021 云服务器密码机技术规范

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 host cryptographic server；cloud-hosted hardware security module；CHSM

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 PCI-E 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 PCI-E 设备(VF)的一种规范。

3.5

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。

3.6

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。

3.7

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。

3.8

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。

3.9

Web 服务　Web service

通过标准的规约进行定义,并通过标准进行访问和使用的一种应用编程接口或 Web 应用编程接口。

4　缩略语

下列缩略语适用于本文件。

API:应用程序接口(Application Program Interface)

CBC:密文分组链接工作模式(Cipher Block Chaining Operation Mode)

CFB:密码反馈工作模式(Cipher Feedback Operation Mode)

CHSM:云服务器密码机(Cloud-hosted Hardware Security Module)

ECB:电码本工作模式(Electronic Codebook Operation Mode)

IV:初始化向量/值(Initialization Vector/Value)

OFB:输出反馈工作模式(Output Feedback Operation Mode)

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

VSM:虚拟密码机(Virtual Security Module)

5　检测环境要求

5.1　常规检测环境

常规检测环境用于检测云服务器密码机的功能,常规检测环境示意图见图 1,性能检测环境示意图见图 2。

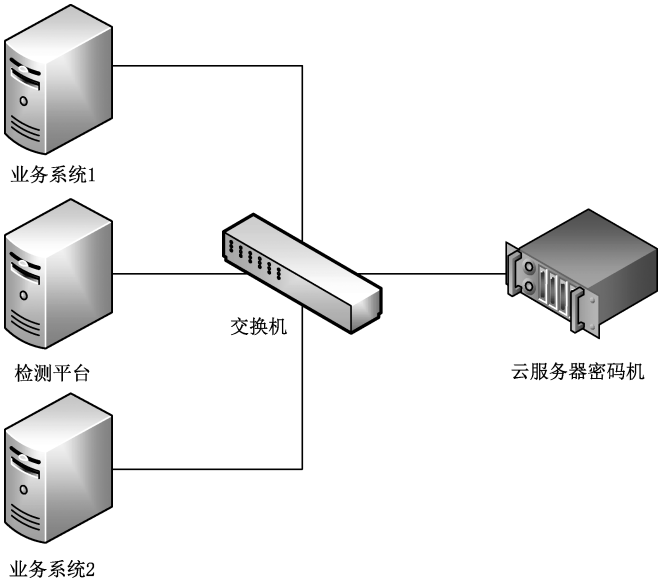

图 1　云服务器密码机常规检测环境拓扑图

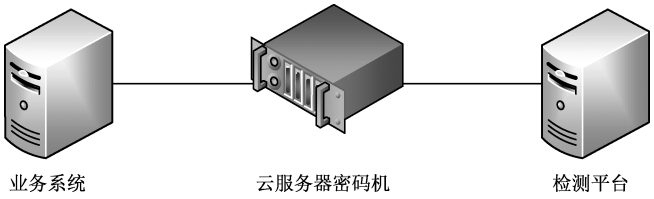

图 2　云服务器密码机性能检测环境拓扑图

5.2　跨网段检测环境

跨网段检测环境用于检测云服务器密码机的跨网段服务能力，跨网段检测环境示意图见图 3。

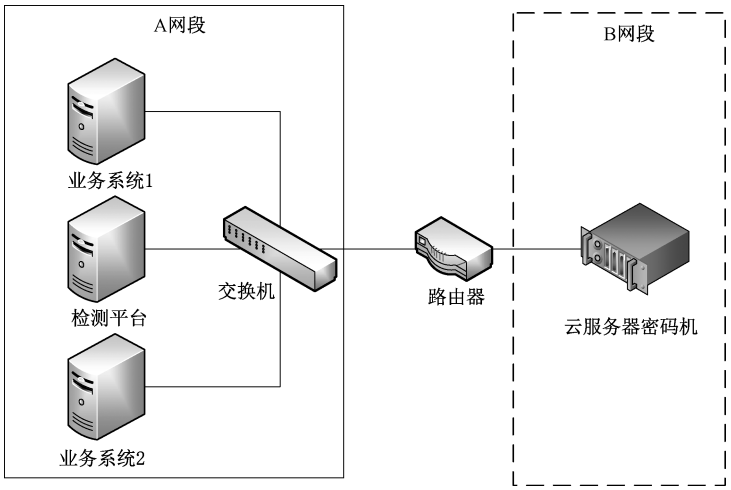

图 3　云服务器密码机跨网段检测环境拓扑图

5.3　云计算检测环境

云计算检测环境用于检测云服务器密码机部署在云计算环境下的服务能力，检测环境拓扑图见

图 4。其中，云平台管理系统负责管理云服务器密码机，管理终端通过云平台管理系统管理云服务器密码机，业务服务器上以虚拟机或容器形式运行业务程序，使用云服务器密码机的密码服务。

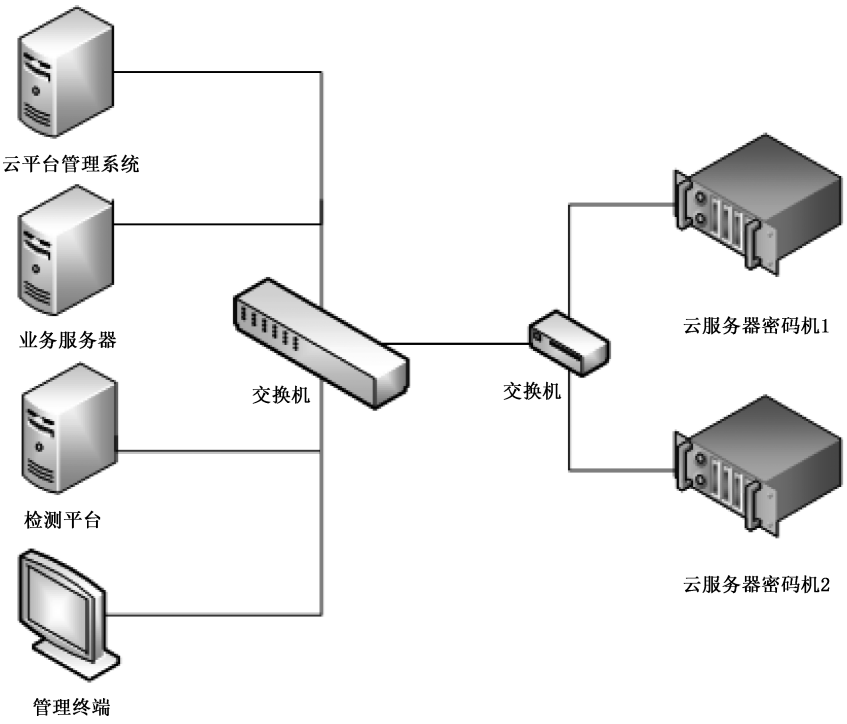

图 4　云服务器密码机云计算检测环境拓扑图

6　检测内容及检测方法

6.1　概述

云服务器密码机检测的主要内容包括 7 项，检测项目列表见附录 A，检测项目包括：

a）　设备外观和结构检查；
b）　功能检测；
c）　安全性检测；
d）　设备网络适应性检测；
e）　性能检测；
f）　环境适应性检测；
g）　可靠性检测。

6.2　设备外观和结构检查

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。

检测内容：

a）　核查云服务器密码机是否具备以下主要部件或接口：
　　1）　应支持状态指示灯，状态灯能区分出正常工作状态和故障状态；
　　2）　应支持至少 2 个网络接口，分别为服务接口和管理接口；
　　3）　应支持电源指示灯，能区分设备是否上电。
b）　核查云服务器密码机是否具备以下主要部件或接口：

1） 宜支持控制口(如:RJ45、DB9、RS232 等);
2） 宜支持冗余电源。

c） 核查云服务器密码机是否具备以下主要部件或接口:
1） 可支持串口;
2） 可支持 USB 接口;
3） 可支持手动密钥销毁开关;
4） 可支持人机交互部件,例如:键盘、显示等。

结果判定:

若 a)结果为肯定,则该检测项为通过。若涉及 b)和 c)项,且结果为肯定,则该检测项为通过。

6.3 功能检测

6.3.1 初始化检测

按照 5.1 进行连接,在云服务器密码机正常启动后,对云服务器密码机应按照 GM/T 0104—2021 中 5.2.2 的规定进行初始化功能检测。

检测内容:

a） 触发宿主机初始化,执行密钥生成(恢复)与安装、生成管理员操作,按照安全机制对密钥进行安全存储和备份,且宿主机能成功进入就绪状态;

b） 触发 VSM 初始化,执行密钥生成(恢复)与安装、生成管理员操作,生成或导入租户和 VSM 的数字证书或标识密码等身份鉴别信息,且 VSM 成功进入就绪状态。

结果判定:

若 a)和 b)结果为肯定,则该检测项为通过。

6.3.2 密码运算检测

云服务器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;使用 SM4 算法应遵循 GB/T 32907,使用 SM2 算法应遵循 GB/T 32918,使用 SM3 算法应遵循 GB/T 32905;宜采用经检测认证的芯片、密码模块、密码卡等作为主要密码部件。

检测内容:

a） 应至少支持 SM4 算法,并提供 ECB、CBC 两种工作模式,宜扩展支持 OFB、CFB 等多种工作模式。VSM 按照指定的工作模式对数据进行加解密运算,检测其运算结果的正确性:
1） 对给定的密钥和明文经对称密码算法 ECB 模式加密,结果和相对应的密文相同;
2） 对给定的密钥和密文经对称密码算法 ECB 模式解密,结果和相对应的明文相同;
3） 对给定的密钥和明文经对称密码算法 CBC 模式加密,结果和相对应的密文相同,其中 IV 值可设定为全 1;
4） 对给定的密钥和密文经对称密码算法 CBC 模式解密,结果和相对应的明文相同,其中 IV 值可设定为全 1;
5） 对给定的密钥和明文经对称密码算法 OFB 模式加密,结果和相对应的密文相同,其中 IV 值可设定为全 1;
6） 对给定的密钥和密文经对称密码算法 OFB 模式解密,结果和相对应的明文相同,其中 IV 值可设定为全 1;
7） 对给定的密钥和明文经对称密码算法 CFB 模式加密,结果和相对应的密文相同,其中 IV 值可设定为全 1;
8） 对给定的密钥和密文经对称密码算法 CFB 模式解密,结果和相对应的明文相同,其中 IV

值可设定为全1。

b) 应至少支持SM2算法，应能够使用SM2算法对数据进行加解密、签名/验签和密钥协商运算，检测其运算结果的正确性：

1) VSM对给定的密钥和明文调用密码算法加密后，检测平台对密文进行解密运算，解密结果和相对应的明文完全相同；

2) 检测平台对给定的密钥和明文调用密码算法加密后，VSM对密文进行解密运算，解密结果和相对应的明文完全相同；

3) VSM对给定的密钥和明文调用密码算法加密后，调用密码算法进行解密运算，解密结果和相对应的明文完全相同；

4) VSM使用给定的密钥对待签名消息调用密码算法签名后，检测平台对签名结果进行验签，验签通过；

5) 检测平台使用给定的密钥对待签名消息调用密码算法签名后，VSM对签名结果进行验签，验签通过；

6) VSM使用给定的密钥对待签名消息调用密码算法签名后，调用密码算法进行验签运算，验签通过；

7) VSM使用给定的密钥和密钥协商参数，调用密钥协商算法与检测平台进行密钥协商，协商结果正确。

c) 应至少支持SM3算法，应能对数据进行杂凑运算，宜支持GB/T 15852.2规定的带密钥的消息鉴别码生成，检测其运算结果的正确性：

1) VSM对给定消息调用SM3算法计算杂凑值，结果和相对应的杂凑值相同；

2) VSM对给定消息和参数调用SM3算法计算杂凑值，结果和给定杂凑值相同，计算过程按GB/T 32905。

结果判定：

若a)中1)～4)、b)、c)中1)结果为肯定，则该检测项为通过。若涉及a)中5)～8)、c)中2)项，且结果为肯定，则该检测项为通过。

6.3.3 密钥管理检测

云服务器密码机应至少支持三层密钥结构，密钥管理包括宿主机和VSM中所有密钥的产生、安装、存储、使用、销毁以及备份和恢复等操作，云服务器密码机的宿主机和各个VSM应使用各自独立的管理工具产生各自的密钥并存储在各自独立的的安全存储区域。云服务器密码机应按照GM/T 0104—2021中6.1的规定进行密钥管理检测。

检测内容：

a) 密钥产生及安装：

1) 私钥和对称密钥的生成中使用的随机数是由商用密码检测认证合格的密码设备或模块产生；

2) 使用指定的参数生成对称或非对称密钥，核查是否能正确存储和使用；

3) 在设备初始化时，宿主机和各VSM使用管理工具成功生成或者安装管理密钥，并以加密或者微电保护方式存储在设备内的安全存储区；

4) 在初始状态，宿主机和各VSM通过管理工具成功生成或安装设备密钥，由各自的管理密钥加密存储，设备密钥对私钥不能以明文形式导出；

5) 在就绪状态，各VSM通过管理工具成功生成和安装用户密钥，私钥以密文等安全形式存储，不能以明文形式导出；

6) 在就绪状态，各VSM通过管理工具成功生成或安装密钥加密密钥，并以密文等安全形式

存储，不能以明文形式导出；

b) 密钥存储与销毁：

1) 核查各个 VSM 是否能够存储至少 32 对非对称密钥和 100 个对称密钥；

2) 核查会话密钥长期存储时，是否使用用户密钥对或密钥加密密钥进行加密保护；

3) 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；

4) 执行密钥销毁时，验证宿主机和 VSM 各自是否能对指定密钥正确置零；

5) 使用微电保护的密钥存储部件，在毁钥触发装置被触发时，是否对所存储的所有密钥正确置零。

c) 密钥使用：

1) 调用密码服务接口，验证租户和应用不能使用设备密钥进行密码运算；

2) 核查除公钥以外的所有密钥均不能以明文形式出现在 VSM 运行空间和安全存储区之外；

3) 核查云服务器密码机是否具备防止非法使用和导出密钥的权限控制机制，验证宿主机不能导出和使用 VSM 的密钥，VSM 不能导出和使用其他 VSM 的密钥；

4) 验证不同的 VSM 是否采用各自的私钥访问控制码进行私钥使用的控制。

d) 密钥备份与恢复：

1) 对持久性保存的密钥，核查云服务器密码机是否具备备份/恢复功能；

2) 执行密钥备份操作，验证产生的备份文件是否以密文形式存储到云服务器密码机外的安全存储介质中，加密备份文件的密钥是否有安全机制保证其安全；

3) 执行密钥恢复操作，验证安全介质中备份的密钥是否能正确恢复到云服务器密码机；

4) 核查宿主机的密钥恢复操作是否只能在宿主机中进行，VSM 的密钥恢复操作是否只能在 VSM 中进行；

5) 核查同厂家的不同型号的云服务器密码机之间是否能够互相备份恢复。

结果判定：

若涉及 b)中 5)和 d)中 5)，且结果为肯定，则该检测项为通过。若其他各项结果为肯定，则该检测项为通过。

6.3.4 随机数质量检测

云服务器密码机应具备随机数生成功能，应至少具备两个独立的经检测认证具有物理噪声源功能的芯片或密码模块，提供随机数生成功能。

检测内容：

a) 随机数质量检测结果应符合 GM/T 0005 的规定，随机数不具备相关性且不能相互推导；

b) 应支持随机数的上电/复位自检、使用自检(包括周期自检和单次自检)和接受指令后的自检，应按照 GM/T 0062 中 E 类产品的要求进行随机数检测；自检失败，应停止提供安全服务，进入错误状态，输出错误指示；

c) 若 VSM 之间共享物理噪声源，核查是否通过虚拟化技术进行逻辑隔离，采用至少两个 VSM 同时进行指定长度随机数生成运算，验证生成的随机数不相同，并对已使用的随机数执行置零操作。

结果判定：

若 a)和 b)结果为肯定，则该检测项为通过。若涉及 c)项，且结果为肯定，则该检测项为通过。

6.3.5 设备管理功能检查

云服务器密码机应按照 GM/T 0104—2021 中 5.2 的规定进行设备管理功能检测。

检测内容：

a) 调用 GM/T 0088 管理接口，验证云服务器密码机的宿主机能否接受云平台管理系统的集中统一管理。

b) 以管理员身份登录宿主机和每个 VSM，验证各管理员的身份鉴别机制和管理的独立性，不同的管理员是否具备不同的操作权限。

c) 验证宿主机的管理员是否无法对 VSM 执行初始化和系统配置、密钥管理等操作。

d) 验证 VSM 的管理员是否无法对宿主机和其他 VSM 执行初始化和系统配置、密钥管理等操作。

e) 验证 VSM 的管理员是否无法执行 VSM 的创建、启动、关闭、删除、漂移等操作。

f) 登录宿主机和每个 VSM 的管理界面，核查远程管理通道和维护通道是否彼此独立，是否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。

g) 核实管理界面是否支持如下管理功能：

1) 支持宿主机和 VSM 的配置、具备管理员的添加和删除等功能；

2) 宿主机的管理员对宿主机进行初始化和系统配置、密钥管理等操作；

3) VSM 的管理员对所属 VSM 进行初始化和系统配置、密钥管理等操作；

4) 宿主机的管理员对 VSM 执行创建、启动、关闭、删除等操作；

5) 宿主机和 VSM 提供日志审计功能，宿主机与 VSM 均提供日志记录、查看、导出等功能；

6) 具备密钥管理功能，包括密钥产生、存储、备份、恢复和销毁等功能；

7) 设备状态管理功能包括设备状态查询功能。

h) 核查管理界面是否具备如下功能：

1) 宿主机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）；

2) 宿主机具备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的功能；

3) 宿主机具备 VSM 的漂移、镜像加载、资源调整等管理操作；

4) 设备状态管理功能包括硬件部件状态、软件状态和版本状态等状态管理功能。

结果判定：

若 a)～g)结果为肯定，则该检测项为通过。若涉及 h)项，且结果为肯定，则该检测项为通过。

6.3.6 设备配置管理检测

云服务器密码机应支持但不限于密码机权限配置、密码机网络配置以及密码机访问控制配置等配置管理功能。

检测内容：

a) 云服务器密码机的宿主机与 VSM 权限配置宜具备：

1) 管理员、安全员、操作员三类角色管理；

2) 管理员负责操作员的添加、修改和注销，以及操作员的权限管理；

3) 安全员负责日志审计；

4) 操作员负责密码机的常规配置操作。

b) 云服务器密码机的宿主机与 VSM 网络配置：

1) 具备密码机本机 IP 地址、掩码以及端口配置，重配置设备宿主机与 VSM 的 IP 地址、掩码及端口，核实网络是否正常连通；

2) 具备密码机网关配置，进行跨网段配置，核实网络是否正常连通。

c) 云服务器密码机的宿主机与 VSM 访问控制配置，可采用 IP 地址访问控制授权表配置，若采用该方式，配置许可 IP 地址，核实是否能获得密码服务。

结果判定：

若 b)结果为肯定，则该检测项为通过。若涉及 a)和 c)，且结果为肯定，则该检测项为通过。

6.3.7 设备自检检测

云服务器密码机应按照 GM/T 0104—2021 中 5.5 的规定进行设备自检功能检测。

检测内容：

a) 查看宿主机开机自检/复位自检日志及接收指令后的自检日志，若涉及以下自检内容，核实日志中是否包含硬件部件自检、物理噪声源的有效性自检、密码运算单元有效性自检、虚拟化功能自检、物理网络检查、数据完整性校验等记录，且记录内容与当前设备的状态相符；

b) 查看 VSM 上电自检/复位自检日志及接收指令后的自检日志，若涉及以下自检内容，核实日志中是否包含密码算法正确性检查、随机数发生器检查、虚拟网络检查、密钥和数据的完整性检查等记录，且记录内容与当前 VSM 的状态相符；

c) 核实自检结果。若自检成功，云服务器密码机宿主机或 VSM 是否进入初始状态或就绪状态；若自检失败，是否记录日志并报警，停止对外提供密码服务；

d) 模拟设备自检检测失败环境，验证是否和预定义的错误一致；

e) 卸载关键部件驱动或删除关键配置文件，进行宿主机或 VSM 开机启动操作，检查开机日志，验证每项的自检结果是否相符，并且密码机无法正常提供管理及密码服务；

f) 登录自检失败的宿主机或 VSM 执行管理员操作或签名等其他密码功能，查看宿主机或 VSM 是否无法进入就绪状态；

g) 登录自检通过的宿主机或 VSM 执行管理员操作，验证宿主机或 VSM 进入相应状态，并且能够正确执行相应操作权限。

结果判定：

若 a)～g)结果为肯定，则该检测项为通过。

6.3.8 设备状态检测

云服务器密码机的设备状态按照 GM/T 0104—2021 中 6.9 的规定的要求检测。

检测内容：

a) 使宿主机和 VSM 处于不同状态，验证宿主机是否具备初始和就绪两个状态，VSM 是否具有初始、就绪和关闭状态；

b) 在宿主机和 VSM 处于初始状态下，验证是否除读取设备信息以及设备密钥的生成或恢复操作外，无法执行任何操作；

c) 在宿主机处于就绪状态下执行登录操作，验证是否鉴别管理员身份之后，方可进行密钥管理操作；

d) 创建 VSM，启动 VSM 并查看 VSM 状态是否是初始状态；

e) 宿主机和 VSM 分别生成或恢复设备密钥，验证宿主机和 VSM 是否均能从初始状态进入就绪状态；

f) 在就绪状态，核查宿主机和 VSM 是否无法执行设备密钥生成和恢复操作；

g) 在就绪状态，核查宿主机和 VSM 是否可以执行除设备密钥生成或恢复以外的任何操作；

h) 向 VSM 发送关闭命令，查看 VSM 是否进入关闭状态；进入关闭状态后，通过调用密码服务核实 VSM 密码服务和对外接口是否关闭，通过查看系统状态核实关键和敏感安全参数是否置零，是否释放所占用的 CPU、内存、IO 接口、持久化存储和密码部件等资源；

i) 向就绪状态的 VSM 发送关闭指令，查看 VSM 是否进入关闭状态；之后向 VSM 发送启动指令，调用密码服务，验证 VSM 是否重新进入就绪状态；

j) 向 VSM 发送停止指令后，查看 VSM 是否进入挂起状态；之后向 VSM 发送启动指令，查看 VSM 是否正常启动并恢复状态；

k) 若具备挂起状态，向 VSM 发送停止命令，查看 VSM 是否进入挂起状态，调用密码服务验证 VSM 是否不能提供密码服务，VSM 管理员是否无法登录 VSM；核查 VSM 的运行时状态信息以及关键和敏感安全参数是否备份后加密存储。

结果判定：

若 a)～i)结果为肯定，则该检测项为通过。若涉及 j)～k)项，且结果为肯定，则该检测项为通过。

6.3.9 服务接口检测

虚拟密码机的服务接口按照 GM/T 0104—2021 中 9.1 的规定的要求检测。

检测内容：

a) 调用 API 服务接口，验证该接口格式是否符合 GM/T 0018 的规定；

b) 若具备 Web 服务接口，验证采用的接口格式与 GM/T 0018 的兼容性；

c) 核查对密码服务调用过程的是否进行身份鉴别、机密性和完整性保护；

d) 若采用传输层密码协议(TLCP)，采集协议交互数据并分析报文格式，验证协议是否实现正确，是否符合 GM/T 0024 的规定；

e) 若采用 IPSec 协议，采集协议交互数据并分析报文格式，验证协议是否实现正确，是否符合 GM/T 0022 的规定；

f) 若采用自定义密码协议，采集协议交互数据并分析报文格式，验证协议是否实现正确，是否符合密码国家标准、行业标准规定。

结果判定：

若 c)结果为肯定，则该检测项为通过。若涉及 a)、b)、d)～f)项，且结果为肯定，则该检测项为通过。

6.3.10 管理接口检测

按照 5.3 进行连接，云服务器密码机的管理接口按照 GM/T 0104—2021 中 9.2 的规定的要求检测。

检测内容：

a) 核查云服务器密码机的管理接口和协议是否符合 GM/T 0088；

b) 启动宿主机管理服务，调用宿主机管理接口，执行 VSM 的创建、启动、关闭、删除、数据影像导入导出等操作，核查云服务器密码机是否能正确响应云平台管理系统的管理和调度；

c) 调用 VSM 的密码运算服务、密钥管理服务的注册、发布、发现、获取和编排接口，对于正确的请求消息报文，VSM 能返回正确的响应消息报文；对于不正确的请求消息报文，VSM 返回的响应消息报文应带有相应的错误代码。

结果判定：

若 a)和 b)结果为肯定，则该检测项为通过。若涉及 c)项，且结果为肯定，则该检测项为通过。

6.3.11 虚拟密码机检测

云服务器密码机的 VSM 按照 GM/T 0104—2021 中 5.7 的规定的要求检测。

检测内容：

a) 验证云服务器密码机是否具备虚拟化功能，是否能通过宿主机管理工具或云平台管理系统接受外部命令，创建、启动、停止、销毁 VSM，检查如下功能：

1) 通过宿主机管理工具或者调用 GM/T 0088 中的“创建 VSM”管理接口，能够在指定的宿

主机上创建新的 VSM；

2） 通过宿主机管理工具或者调用 GM/T 0088 中的“启动 VSM”管理接口，能够在指定的宿主机上启动指定的 VSM；

3） 通过宿主机管理工具或者调用 GM/T 0088 中的“停止 VSM”管理接口，能够在指定的宿主机上停止指定的 VSM；

4） 通过宿主机管理工具或者调用 GM/T 0088 中的“删除 VSM”管理接口，能够在指定的宿主机上销毁指定的 VSM。

b） 核查云服务器密码机是否具备密钥隔离功能：是否能防止 VSM 的密钥被盗用、防止 VSM 之间交叉使用密钥、防止宿主机管理员获取 VSM 密钥。

c） 验证 VSM 的镜像文件是否进行了签名保护。

d） 登录云平台管理系统，查看云服务器密码机是否支持定义并向云平台管理系统上报支持的最大 VSM 数量。

e） 执行 VSM 漂移，验证 VSM 的数据影像是否具备加密和完整性保护功能。

f） 执行对 VSM 的处理器、内存、网络、密码运算、密钥存储等资源的调整功能，查看调整结果是否与预期一致。

结果判定：

若 a)～c)结果为肯定，则该检测项为通过。若涉及 d)～f)项，且结果为肯定，则该检测项为通过。

6.3.12 设备访问控制与身份鉴别检测

云服务器密码机设备访问控制与身份鉴别检测按照 GM/T 0104—2021 中 6.2 的规定的要求检测。

检测内容：

a） 分析宿主机和管理员之间、VSM 和管理员之间、使用 VSM 的租户/应用和 VSM 之间的身份鉴别数据，查看是否实现身份的双向鉴别功能；管理员和用户是否采用了基于数字证书、标识密码或硬件身份介质等实现身份鉴别机制，并符合 GM/T 0028 安全二级及以上的要求；

b） 以不同宿主机或 VSM 的用户身份登录，查看是否具备不同的操作权限；

c） 验证是否使用私钥访问控制码对存储在 VSM 内部的私钥进行有效控制；

d） 对 VSM 服务接口进行调用和对宿主机和 VSM 进行远程管理，验证是否采用基于 IP 地址的授权访问控制技术；

e） 验证 VSM 是否只能由其自身的管理员单独对其访问进行授权。

结果判定：

若 a)～e)结果为肯定，则该检测项为通过。

6.3.13 设备日志记录检测

云服务器密码机设备日志记录按照 GM/T 0104—2021 中 5.4 的规定的要求检测。

检测内容：

a） 分别登录宿主机和每个 VSM 管理员，查看日志记录，核实是否独立存储和操作；

b） 执行管理员登录认证、系统配置、密钥管理等操作，查看宿主机和 VSM 是否有各自的操作日志记录；

c） 宿主机对 VSM 执行创建、启动、关闭、删除、漂移等操作，查看是否记录该操作或事件及其结果；

d） 宿主机和 VSM 执行认证失败、非法访问等异常事件，查看是否保存异常日志记录；

e） 宿主机接受云平台管理系统的相应管理命令及操作，查看是否记录该操作或事件及其结果；

f） 管理员登录，验证日志查看、日志导出等操作是否成功；

g） 进行日志审计，验证是否具有关键日志记录的完整性校验或其他防篡改功能。

结果判定：

若 a）～g）结果为肯定，则该检测项为通过。

6.3.14 安全隔离检测

云服务器密码机的 VSM 之间、VSM 和宿主机之间应实现安全隔离，不准许相互访问。VSM 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。云服务器密码机应至少支持管理隔离、使用隔离、系统隔离、密码部件隔离、网络隔离和密钥隔离功能。安全隔离按照 GM/T 0104—2021 中 6.7 的规定的要求检测。

检测内容：

a） 管理隔离：

1） 执行宿主机与 VSM 网络配置，核查宿主机和不同的 VSM 是否具备不同的管理 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；

2） 使用来自同一 IP 的终端设备同时登录宿主机和不同的 VSM，验证是否无法登录；

3） 分别登录宿主机和 VSM，验证宿主机和不同的 VSM 之间是否无法共享用户信息，能否进行完全独立的用户管理；

4） 核查宿主机和不同的 VSM 是否具备独立的管理界面和管理员。

结果判定：若 1）～4）结果为肯定，则该检测项为通过。

b） 使用隔离：

1） 启用对外密码服务，查看不同的 VSM 是否采用不同的服务 IP 地址、服务域名或服务端口并采用不同的安全通道；

2） 分别进入宿主机和不同 VSM 系统内，查看访问密码部件的进程信息是否不同、用于访问密码部件的标识信息是否不同；

3） 当采用软件或固件模块提供密码运算时，查看宿主机和不同的 VSM 是否分配了不同的 CPU 物理核。

结果判定：若 1）～3）结果为肯定，则该检测项为通过。

c） 系统隔离：

1） 核查是否为经过论证的可用的安全隔离技术；

2） 核查网络协议栈、文件系统、进程空间和用户空间等系统资源的封装和隔离是否有效；

3） 核查 VSM 是否占用独立的 CPU 处理核；

4） 核查运行中的 VSM 是否使用专属内存；

5） 登录进入 VSM 系统，验证是否不能查看其他 VSM 的系统信息、文件和进程，是否不能访问到其他 VSM；

6） 核查不同 VSM 的持久性存储区域是否采用加密文件系统或文件/目录访问控制等技术进行安全隔离保护；

7） 如果采用加密文件系统方式，验证不同 VSM 是否采用不同的密钥加密保护持久性存储区域；如果采用文件/目录访问控制方式，查看不同 VSM 是否采用不同的文件/目录进行持久性存储。

结果判定：若 1）和 2）结果为肯定，则该检测项为通过。若涉及 3）～7）项，且结果为肯定，则该检测项为通过。

d） 密钥隔离：

1） 核查宿主机和不同 VSM 是否具备各自独立的密钥管理功能，核查宿主机是否具备管理

密钥、设备密钥，各个 VSM 是否具有各自的管理密钥、设备密钥、用户密钥、密钥加密密钥和会话密钥，宿主机和 VSM 是否各自具备独立的密钥管理功能，且密钥结构符合 GM/T 0104—2021 中 6.1.2 的要求；

2) 核查云服务器密码机的顶层密钥是否符合 GM/T 0104—2021 中 6.1.4 的要求；

3) 管理员登录宿主机和 VSM，验证宿主机和不同 VSM 的管理密钥是否采用不同的授权码（管理员口令或智能密码钥匙的 PIN 码等）进行存储和访问控制；

4) 核查宿主机管理密钥的授权码是否由宿主机管理员保管和使用，不同 VSM 管理密钥的授权码由各自租户管理员保管和使用。使用同一授权码访问多个 VSM，验证 VSM 的密钥隔离机制的有效性。

结果判定：若 1)～4)结果为肯定，则该检测项为通过。

e) 密码部件隔离：

1) 核查密码运算部件、密钥存储部件、随机数发生器等密码部件是否采用物理或逻辑方式为宿主机和不同 VSM 划分不同的运算单元和存储空间；

2) 检查是否为宿主机和不同 VSM 划分不同的数据和控制命令传输通道：

——密码部件的 IO（输入输出）接口若采用基于硬件的虚拟化技术，进入不同 VSM 系统内，核查是否为不同的 VSM 分配了独立的虚拟密码部件（VF），并能够查看 VF 的 id 信息；

——密码部件的 IO（输入输出）接口若采用基于软件的虚拟化技术，设备驱动程序或 API 内部应具有访问控制手段；

3) 如果采用基于硬件的虚拟化技术对设备的密码部件在 VSM 之间进行安全隔离与共享，则进入不同 VSM 系统内，核查是否为不同的 VSM 分配了独立的虚拟密码部件（VF），并能够查看 VF 的 id 信息；

4) 如果采用基于软件的虚拟化技术对设备的密码部件在 VSM 之间进行安全隔离与共享，则进入不同 VSM 系统内，核查是否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，是否通过为不同的 VSM 分配不同的设备句柄或任务 ID 进行 VSM 的区分和隔离。

结果判定：若 1)和 2)结果为肯定，则该检测项为通过。若涉及 3)～4)项，且结果为肯定，则该检测项为通过。

f) 网络隔离：

1) 核查是否采用基于硬件或软件的虚拟化技术对设备的网络接口在 VSM 之间进行安全隔离与共享；

2) 当采用 SRIOV 等硬件虚拟化技术进行网络接口的共享时，核查是否为不同的 VSM 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；

3) 当不采用 SRIOV 等硬件虚拟化技术进行网络接口的共享时，核查通过软件实现的虚拟交换机进行不同 VSM 的网络隔离，不同的虚拟网络接口应具有不同的 MAC 地址。

结果判定：

若 1)结果为肯定，则该检测项为通过。若涉及 2)～3)项，且结果为肯定，则该检测项为通过。

结果判定：

若 a)～f)结果为通过，则该检测项为通过。

6.4 安全性检测

云服务器密码机应保证不存在已知漏洞。云服务器密码机的设备安全性检测按照 GM/T 0039 和 GM/T 0104—2021 中 6.4、6.5 的规定的要求检测。

检测内容：

a) 核查云服务器密码机的硬件是否符合 GM/T 0028 的硬件安全要求；

b) 核查云服务器密码机的软件和固件是否符合 GM/T 0028 的软件/固件的安全二级要求；

c) 核查设备结构，是否具有支持防拆、防撬结构设计，如：采用全密封机壳、物理锁控制开启面板；

d) 核查云服务器密码机的操作系统是否进行安全加固，裁剪一切不需要的功能，关闭所有不需要的端口和服务；

e) 送检单位承诺产品中不存在已知安全漏洞，并提供最近的漏洞扫描报告；

f) 核查是否具备紧急情况下人工毁钥装置。

结果判定：

若 a)～e)结果为肯定，则该检测项为通过。若涉及 f)项，且结果为肯定，则该检测项为通过。

6.5 设备网络适应性检测

云服务器密码机对使用主体的服务模式应至少满足三种模式的应用要求，包括：

a) 应能够与使用云服务器密码机的设备直接连接使用，连接方式按照 5.1 进行；

b) 应能够通过交换机同时与多台使用云服务器密码机的设备连接使用，连接方式按照 5.1 进行；

c) 应能够与不同网段使用云服务器密码机的设备连接使用，连接方式按照 5.2 进行。

6.6 性能检测

6.6.1 通则

按照 5.1 进行连接，检测云服务器密码机的 VSM 数量以及进行各项密码运算的性能指标。

云服务器密码机的性能检测应包括八方面：随机数产生性能、对称密钥产生性能、非对称密钥对产生性能、对称密码算法加解密性能、非对称密码算法加解密性能、非对称密码算法签名及验签性能、杂凑算法运算性能、VSM 最大数量。

密码算法各项性能检测，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 VSM 并将所有计算资源分配给该 VSM 时，该 VSM 的各项性能检测数据；满负载指创建和启动该云服务器密码机支持的最大数量 VSM 并对所有 VSM 并行进行各项性能检测时，所有 VSM 的各项性能检测数据之和、平均数据、单个最大及单个最小数据。测试应至少进行三次以上，结果取平均值。

6.6.2 虚拟密码机最大数量检测

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，单位为个。

6.6.3 对称密码算法加解密性能检测

检测 SM4 算法所支持的工作模式（至少包括 ECB、CBC 两种工作模式）中性能最高的模式下加/解密速度；将一个长度为 L（字节）的数据报文，发送给虚拟密码机进行加/解密操作，重复操作 N 次（N 不小于 1 000 次），测量其完成时间 T（秒）。公式为：

$$S = 8LN/(1\,024 \times 1\,024T) \qquad \cdots\cdots(1)$$

式中：

S ——速度，单位为兆比特每秒（Mb/s）；

L ——数据报文的长度，单位为字节（B）；

N——测试次数；

T——测量所耗费的时间，单位为秒(s)。

6.6.4 非对称密码算法加解密性能检测

检测 SM2 算法的加密/解密速度；将一个长度为 L(字节)的数据报文发送给虚拟密码机进行签名/验证操作，重复操作 N 次(如：1 000 次)，测量其完成时间 T(秒)。公式为：

$$S = 8LN/(1\ 024 \times 1\ 024T) \quad \cdots\cdots(2)$$

式中：

S——速度，单位为兆比特每秒(Mb/s)；

L——数据报文的长度，单位为字节(B)；

N——测试次数；

T——测量所耗费的时间，单位为秒(s)。

6.6.5 非对称密码算法签名验证性能检测

检测 SM2 算法的签名/验证速度；将一个定长的数据报文，发送给虚拟密码机进行签名/验证操作，重复操作 N 次(如：1 000 次)，测量其完成时间 T(秒)。公式为：

$$S = N/T \quad \cdots\cdots(3)$$

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)。

6.6.6 杂凑算法运算性能检测

检测 SM3 算法运算速度；将一个长度为 L(字节)的数据报文，发送给虚拟密码机进行摘要运算，重复操作 N 次(如：1 000 次)，测量其完成时间 T(秒)。公式为：

$$S = 8LN/(1\ 024 \times 1\ 024T) \quad \cdots\cdots(4)$$

式中：

S——速度，单位为兆比特每秒(Mb/s)；

L——数据报文的长度，单位为字节(B)；

N——测试次数；

T——测量所耗费的时间，单位为秒(s)。

6.6.7 随机数产生性能检测

检测随机数的产生速度；让虚拟密码机生成并输出长度为 L(字节)的符合随机特性的随机序列 N 组(如：1 000 组)，测量其完成时间 T(秒)。公式为：

$$S = 8LN/(1\ 024 \times 1\ 024T) \quad \cdots\cdots(5)$$

式中：

S——速度，单位为兆比特每秒(Mb/s)；

L——数据报文的长度，单位为字节(B)；

N——随机序列组数；

T——测量所耗费的时间，单位为秒(s)。

6.6.8 对称密钥产生性能检测

检测对称密钥生成速度；让虚拟密码机生成并输出 M 个(如：1 000 个)128 bit 密钥，测量其完成时

间 T(秒)。公式为：

$$S=M/T \quad \cdots\cdots(6)$$

式中：

S ——速度，单位为次每秒(次/s)；

M——输出密钥的个数；

T ——测量所耗费的时间，单位为秒(s)。

6.6.9 非对称密钥对产生性能检测

检测非对称密钥对生成速度，让虚拟密码机生成并输出 M 对(如：1 000 对)密钥对，测量其完成时间 T(秒)。公式为：

$$S=M/T \quad \cdots\cdots(7)$$

式中：

S ——速度，单位为对每秒(对/s)；

M——输出密钥对的对数；

T ——测量所耗费的时间，单位为秒(s)。

6.7 环境适应性检测

云服务器密码机设备环境适应性检测应达到 GM/T 0104—2021 中 7.3 的要求。

6.8 可靠性检测

云服务器密码机设备可靠性检测应达到 GM/T 0104—2021 中 7.4 的要求。

7 送检技术文档要求

研制单位按照商用密码检测认证机构要求提交相关文档资料及虚拟化技术安全自测试报告，作为云服务器密码机的检测依据。

8 判定规则

6.2～6.5 的各项检测中，所有项目检测结果判定为“通过”，则判定为产品合格，否则，产品不合格。

附 录 A
（资料性）
检测项目列表

设备外观及结构检查见表 A.1。

表 A.1 设备外观及结构检查

检测项目	检 测 子 项 目
设备外观	状态指示灯
	电源指示灯
	手动密钥销毁开关
	接口
	冗余电源
	人机交互部件
	外观和尺寸

初始化检测见表 A.2。

表 A.2 初始化检测

检测项目	检 测 子 项 目
初始化	宿主机的密钥生成(恢复)与安装、生成管理员、密钥的安全存储和备份
	虚拟机的密钥生成(恢复)与安装、生成管理员、密钥的安全存储和备份
	虚拟机租户和对应虚拟密码机身份鉴别信息的生成或导入

密码运算检测见表 A.3。

表 A.3 密码运算检测

检测项目	检 测 子 项 目
SM2 密码运算检测	给定密钥和明文进行 SM2 算法公钥加密
	给定密钥和密文进行 SM2 算法私钥解密
	给定的密钥和签名值进行 SM2 算法验证签名
	给定的密钥和明文进行 SM2 算法签名
	给定密钥和密钥协商参数进行 SM2 算法密钥协商产生会话密钥
SM3 密码运算检测	给定明文和参数进行 SM3 算法计算杂凑值

表 A.3　密码运算检测（续）

检测项目	检 测 子 项 目
SM4 密码运算检测	给定密钥和明文 SM4 算法 ECB 模式加密
	给定密钥和密文 SM4 算法 ECB 模式解密
	给定密钥和明文 SM4 算法 CBC 模式加密
	给定密钥和密文 SM4 算法 CBC 模式解密
	给定密钥和明文 SM4 算法 OFB 模式加密
	给定密钥和密文 SM4 算法 OFB 模式解密
	给定密钥和明文 SM4 算法 CFB 模式加密
	给定密钥和密文 SM4 算法 CFB 模式解密

密钥管理检测见表 A.4。

表 A.4　密钥管理检测

检测项目	检 测 子 项 目
密钥管理	密钥产生及安装
	密钥存储与销毁
	密钥使用
	密钥备份与恢复

随机数质量检测见表 A.5。

表 A.5　随机数质量检测

检测项目	检 测 子 项 目
随机数质量检测	随机数质量检测
	随机数自检功能
	随机数生成机制安全性测评

设备管理功能检测见表 A.6。

表 A.6　设备管理功能检测

检测项目	检 测 子 项 目
管理功能	向云平台管理系统注册及接受管理操作
	管理员身份鉴别及管理独立性(宿主机和 VSM)
	远程管理通道和维护通道独立性
	管理界面功能

设备配置管理检测见表 A.7。

表 A.7　设备配置管理检测

检测项目	检 测 子 项 目
配置管理	宿主机与 VSM 权限配置
	宿主机与 VSM 网络配置
	宿主机与 VSM 访问控制配置

设备自检检测见表 A.8。

表 A.8　设备自检检测

检测项目	检 测 子 项 目
设备自检	上电/复位、周期、单次和接受指令自检
	自检成功自动进入初始化配置或就绪状态
	自检失败报告检测结果

设备状态检测见表 A.9。

表 A.9　设备状态检测

检测项目	检 测 子 项 目
设备状态	初始态
	就绪态
	挂起状态
	关闭状态
	状态转换

设备服务接口检测见表 A.10。

表 A.10　设备服务接口检测

检测项目	检 测 子 项 目
设备服务接口	API 服务接口
	Web 服务接口
	密码服务调用过程中传输层消息安全性
	传输层密码协议(TLCP)
	IPSec 协议
	自定义密码协议

管理接口检测见表 A.11。

表 A.11　设备管理接口检测

检测项目	检 测 子 项 目
管理接口	云服务器密码机管理接口和协议
	对云平台管理系统管理和调度的响应
	VSM 响应消息报文正确性

虚拟密码机检测见表 A.12。

表 A.12　虚拟密码机检测

检测项目	检 测 子 项 目
虚拟密码机	虚拟化
	密钥隔离
	镜像文件
	VSM 数目
	VSM 的数据影像
	VSM 占用资源

设备访问控制与身份鉴别检测见表 A.13。

表 A.13　设备访问控制与身份鉴别检测

检测项目	检 测 子 项 目
设备访问控制与身份鉴别	宿主机与其管理员的身份鉴别机制
	VSM 和其管理员的身份鉴别机制
	VSM 的租户/应用和 VSM 之间的身份鉴别机制
	不同身份操作权限
	私钥访问控制码
	基于 IP 地址的授权访问控制技术

设备日志记录检测见表 A.14。

表 A.14　设备日志记录检测

检测项目	检 测 子 项 目
设备日志记录	日志记录
	日志查看/导出
	日志审计

安全隔离检测见表 A.15。

表 A.15　安全隔离检测

检测项目	检 测 子 项 目
安全隔离	管理隔离
	使用隔离
	系统隔离
	密钥隔离
	密码部件隔离
	网络隔离

安全性检测见表 A.16。

表 A.16　安全性检测

检测项目	检 测 子 项 目
设备安全性	硬件安全
	软件和固件安全
	VSM 安全
	操作系统安全

设备网络适应检测见表 A.17。

表 A.17　设备网络适应检测

检测项目	检 测 子 项 目
设备网络适应	使用云服务器密码机的设备直连
	局域网连接
	跨网段连接使用

性能检测见表 A.18。

表 A.18　性能检测

检测项目	检 测 子 项 目
设备性能	虚拟密码机最大数量
	对称密码算法加解密性能
	非对称密码算法加解密性能
	非对称密码算法签名/验证性能
	杂凑算法运算性能
	随机数产生性能
	对称密钥产生性能
	非对称密钥对产生性能

环境适应性检测见表 A.19。

表 A.19　环境适应性检测

检测项目	检 测 子 项 目
设备日志记录	对设备环境适应性检测达到 GM/T 0104—2021 中 7.3 的要求

可靠性检测见表 A.20。

表 A.20　可靠性检测

检测项目	检 测 子 项 目
设备日志记录	对设备可靠性检测达到 GM/T 0104—2021 中 7.4 的要求

中华人民共和国密码
行业标准
云服务器密码机检测规范
GM/T 0142—2024
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 2　字数 44 千字
2025年6月第1版　2025年6月第1次印刷
*
书号:155066·2-39081　定价 54.00 元

GM/T 0142-2024