ICS 35.040
L 80
备案号：

中华人民共和国密码行业标准

GM/T 0059—2018

服务器密码机检测规范

Cryptographic server test specifications

（报批稿）

2018-05-02 发布　　2018-05-02 实施

国家密码管理局 发布

目　次

前　言

本标准依照 GB/T1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：卫士通信息产业股份有限公司、国家密码管理局商用密码检测中心、无锡江南信息安全工程技术中心、兴唐通信科技股份有限公司、山东得安信息技术有限公司。

本标准主要起草人：刘平、罗俊、胡显荃、李元正、张世雄、邓开勇、罗鹏、刘常、李国友、肖秋林、徐强、徐明翼、王妮娜、王海霞、孔凡玉、郑海森。

本标准凡涉及密码算法相关内容，按国家有关法规实施。

服务器密码机检测规范

1 范围

本标准规定了服务器密码机类密码设备的检测要求和检测方法。

本标准适用于服务器密码机类密码设备的检测，以及该类密码设备的研制，也可用于指导基于该类密码设备的应用开发。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件，凡是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 微型计算机通用规范

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 32915 信息安全技术 二元序列随机性检测规范

GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 33560 信息安全技术 密码应用标识规范

GM/T 0009-2012 SM2 密码算法使用规范

GM/T 0018-2012 密码设备应用接口规范

GM/T 0028-2014 密码模块安全技术要求

GM/T 0030-2014 服务器密码机技术规范

GM/T 0039-2015 密码模块安全检测要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

服务器密码机 Cryptographic Server

又称主机加密服务器，能独立或并行为多个应用实体提供密码服务和密钥管理的设备。

3.2

非对称密码算法/公钥密码算法 Asymmetric Cryptographic Algorithm/Public Key Cryptographic Algorithm

加解密使用不同密钥的密码算法。

3.3

对称密码算法 symmetric cryptographic algorithm

加密和解密使用相同密钥的密码算法。

3.4

分组密码算法 block cipher algorithm

将输入数据划分成固定长度的分组进行加解密的一类对称密码算法。

3.5

加密 Encipherment/Encryption

对数据进行密码变换以产生密文的过程。

3.6

解密 Decipherment/Decryption

加密过程对应的逆过程。

3.7

设备密钥 Device Key Pair

存储在设备内部的用于设备管理的非对称密钥对，包含签名密钥对和加密密钥对。

3.8

公钥基础设施 Public Key Infrastructure

用公钥密码技术建立的普遍适用的基础设施，为用户提供证书管理和密钥管理等安全服务。

3.9

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。

3.10

SM1 算法 SM1 algorithm

一种分组密码算法。

3.11

SM2 算法 SM2 algorithm

由 GB/T 32918《信息安全技术 SM2 椭圆曲线公钥密码算法》定义的一种算法。

3.12

SM3 算法 SM3 algorithm

由 GB/T 32905《信息安全技术 SM3 密码杂凑算法》定义的一种算法。

3.13

SM4 算法 SM4 algorithm

由 GB/T 32907《信息安全技术 SM4 分组密码算法》定义的一种算法。

4 符号和缩略语

下列缩略语适用于本文件。

API　　应用程序接口(Application Program Interface)

CBC　　（分组密码的）密码分组链接（工作方式）(Cipher Block Chaining)

CFB　　（分组密码的）密码反馈（工作方式）(Cipher Feedback)

CS　　服务器密码机（Cryptographic Server）

ECB　　（分组密码的）电子密本（工作方式）(Electronic Codebook)

OFB　　（分组密码的）输出反馈（工作方式）(Output Feedback)

5 检测环境要求

5.1 常规检测环境

服务器密码机常规检测环境用于检测服务器密码机的功能、性能，检测环境拓扑可参考图 1。

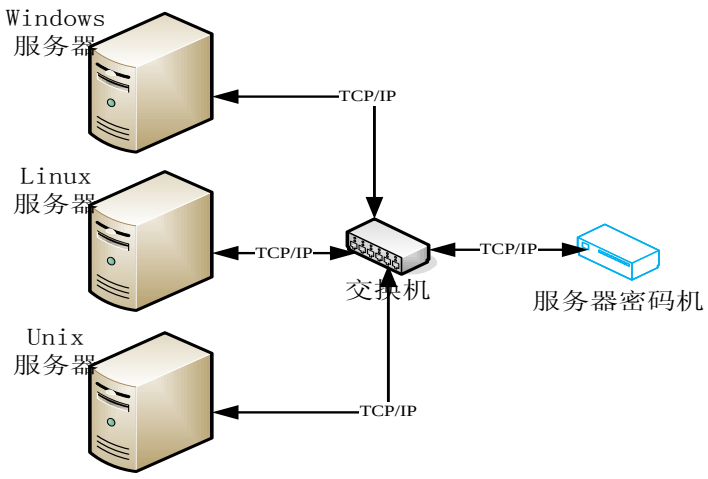

图 1　服务器密码机常规检测环境拓扑图

5.2　跨网段检测环境

服务器密码机跨网段检测环境用于检测服务器密码机的跨网段服务能力，检测环境拓扑可参考图 2。

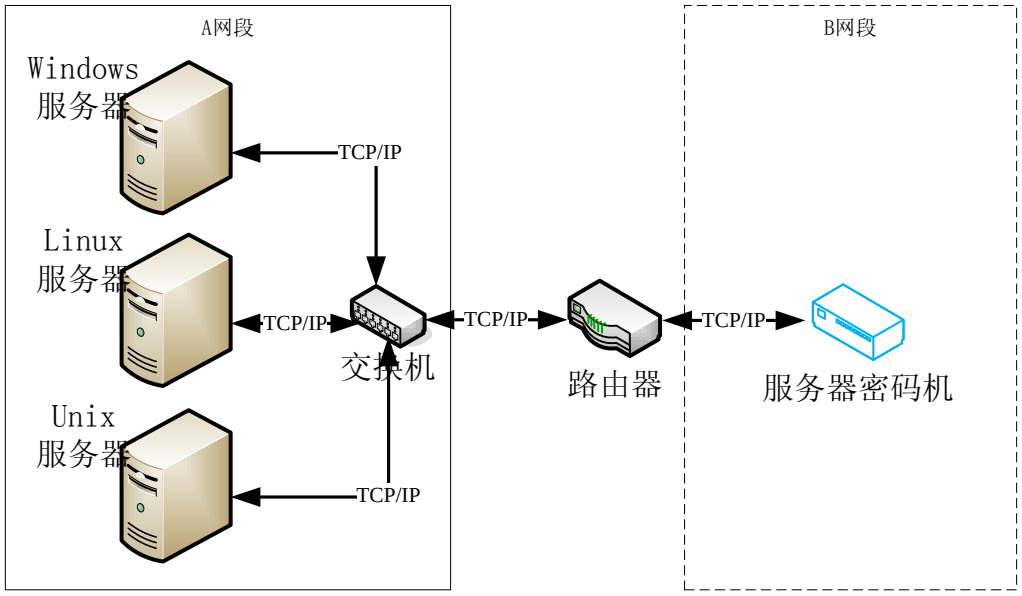

图 2　服务器密码机跨网段检测环境拓扑图

6　检测内容

6.1　概述

本标准相关检测内容包括但不限于 GM/T 0030-2014 第 9 章内容，服务器密码机检测的主要内容包括 20 项，检测项目列表参见附录 A，检测项目包括：

a)　设备外观及结构检查；

b)　设备管理功能检查；

c) 设备状态检测；
d) 设备自检检测；
e) 设备配置管理检测；
f) 设备密钥管理检测；
g) 设备 SM1 密码运算检测；
h) 设备 SM2 密码运算检测；
i) 设备 SM3 密码运算检测；
j) 设备 SM4 密码运算检测；
k) 设备随机数质量检测；
l) 设备应用接口检测；
m) 设备管理接口检测；
n) 设备访问控制检测；
o) 设备日志记录检测；
p) 设备性能检测；
q) 设备网络适应性检测；
r) 设备安全性检测；
s) 设备环境适应性检测；
t) 设备可靠性检测。

6.2 设备外观及结构检查

服务器密码机应具备以下主要部件或接口：
a) 应支持状态指示灯，目测状态灯能区分出正常工作状态和故障状态；
b) 应支持电源指示灯，目测能区分设备是否上电；
c) 应支持至少 2 个 RJ45 网络接口。
服务器密码机宜具备以下主要部件或接口：
a) 宜支持 1 个串口（RJ45 或 DB9 形态）作为控制口；
b) 宜支持冗余电源。
服务器密码机可具备以下主要部件或接口：
a) 可支持手动密钥销毁开关；
b) 可支持 DB9 串口；
c) 可支持 USB 接口；
d) 可支持人机交互部件，例如：键盘、显示器等。

6.3 设备管理功能检查

服务器密码机应支持管理功能和密码服务功能，不同功能采用分开的物理接口访问，例如：管理功能使用网络接口 1 访问，则密码服务功能应采用网络接口 2 访问。服务器密码机采用远程管理方式时，管理机与密码机之间应建立安全通道。

管理界面应支持下面几个主要管理功能：
a) 应支持密钥管理功能，密钥管理功能应包括密钥产生、密钥存储、密钥备份、密钥恢复和密钥销毁等子功能；
b) 应支持设备唯一标识符查询；
c) 应支持设备状态管理功能，设备状态管理应包括设备状态查询功能，宜包括硬件部件状态、软件状态和版本状态等状态管理功能。

管理界面宜包含下面几个主要管理功能：

a) 宜支持网络地址配置功能，网络地址配置功能宜包含 IP 地址、子网掩码以及网关地址等网络参数配置功能；
b) 宜支持日志管理，日志管理功能宜包含日志记录、日志查询和日志导出等功能。

6.4 设备状态检测

服务器密码机应具备初始状态和就绪状态两种状态，且只能由初始状态向就绪状态转换。

服务器密码机首次加电启动，应自动进入初始状态，此时密码机不能提供密码服务。由用户执行密码机的初始化配置，初始化配置应包含用户管理、密钥管理、系统配置，待各项配置完成后应重新启动密码机。

经过初始化配置的密码机加电启动，可自动进入就绪状态，密码机方可提供密码服务。

就绪状态的密码机只能通过触发毁钥机制并断电重启后，才能再次进入初始状态，不能通过管理界面、控制口、人机交互部件或其它方式将密码机的状态从就绪状态转换到初始状态。

6.5 设备自检检测

服务器密码机应支持自检功能，自检应包括上电/复位自检、周期自检和接受指令后的自检，自检内容包括物理噪声源有效性自检、密码运算单元有效性自检、随机数自检、密码算法正确性自检、静态存储数据的完整性校验等。

自检结束后应报告检测结果。自检成功，密码机应进入就绪状态；自检失败，密码机应记录日志并报警，并立即停止对外提供密码服务。

6.6 设备配置管理检测

服务器密码机应包含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管理功能。

密码机权限配置宜具备：

a) 管理员、安全员、操作员三类角色管理；
b) 管理员负责安全员和操作员的添加、修改和注销；
c) 安全员负责操作员的权限管理以及日志审计；
d) 操作员负责密码机的常规配置操作。

密码机网络配置宜具备：

a) 密码机本机 IP 地址、掩码以及端口配置；
b) 密码机网关配置。

密码机访问控制配置宜具备：

a) IP 地址访问控制授权表的配置；
b) 内部存储私钥的权限标识码的配置。

6.7 设备密钥管理检测

6.7.1 密钥管理安全措施

服务器密码机应具备完善的密钥管理功能，应至少支持三层密钥结构。密钥管理包括密钥产生、安装、存储、使用、更换、销毁以及备份和恢复等功能，密码机应保证密钥在生存周期的各个环节的安全性。

服务器密码机应具备以下密钥安全保护措施：

a) 应支持按照指定的参数生成非对称密钥对并安全地存储在密码机内部；

b) 应采用访问控制技术控制内部存储密钥的访问和使用；
c) 应提供销毁内部存储密钥的措施；
d) 应支持以安全的方法备份内部存储密钥到安全介质；
e) 应支持以安全的方法将安全介质中备份的密钥恢复到密码机；
f) 应支持通过备份介质安全地将密钥同步至另一台相同的设备；
g) 应支持内部存储的非对称密钥对的公钥能被导出到密码机外使用。

6.7.2 密钥管理安全功能

服务器密码机应符合 GM/T 0030 标准，具备以下密钥管理安全功能：

a) 管理密钥应在初始态由服务器密码机厂家提供的管理工具生成或安装，且安全地存储在密码机内部；
b) 用户密钥和设备密钥的签名密钥对由服务器密码机生成或安装，密钥所使用的的随机数应使用物理噪声源芯片生成，密钥的生成应使用强素数；加密密钥对由独立的密钥管理系统产生并按照GM/T 0018中规定的加密密钥对私钥保护结构下发到设备中；
c) 密钥加密密钥是可选择支持项，当密码机支持此项时，该密钥应由服务器密码机厂家提供的管理工具生成或安装并应支持在密码机内部安全地存储一定数量的密钥加密密钥；
d) 会话密钥不能明文导出，导出时应使用用户密钥或密钥加密密钥加密；
e) 密码机中安全存储的对称密钥和非对称密钥应以密钥索引号或其他形式的唯一标识进行调用；
f) 密码机应可安全存储至少 100 组对称密钥和 32 对非对称密钥对；
g) 密码机应支持密钥备份和密钥恢复，备份文件应以密文形式存放在安全的存储介质中，且同厂家的同型号密码机应能够支持相互间进行备份和恢复。

6.8 设备密码算法正确性与一致性检测

6.8.1 设备对称密码运算检测

服务器密码机应支持 SM4 分组密码算法，可支持 SM1 分组密码算法，对每种算法应提供 ECB、CBC 二种工作模式，也可扩展支持 OFB、CFB 等工作模式。

服务器密码机应能按照指定的工作模式对数据进行加解密运算。应能支持各模式下分别给定密钥和明文（密文），检测其运算结果的正确性，包括：

a) 密码机对给定的密钥和明文经 ECB 模式加密，结果和给定密文完全相同；
b) 密码机对给定的密钥和密文经 ECB 模式解密，结果和给定明文完全相同；
c) 密码机对给定的密钥和明文经 CBC 模式加密，结果和给定密文完全相同；
d) 密码机对给定的密钥和密文经 CBC 模式解密，结果和给定明文完全相同；
e) 密码机对给定的密钥和明文经 OFB 模式加密，结果和给定密文完全相同；
f) 密码机对给定的密钥和密文经 OFB 模式解密，结果和给定明文完全相同；
g) 密码机对给定的密钥和明文经 CFB 模式加密，结果和给定密文完全相同；
h) 密码机对给定的密钥和密文经 CFB 模式解密，结果和给定明文完全相同。

6.8.2 设备非对称密码运算检测

服务器密码机应支持SM2公钥密码算法。密码机应能够使用SM2算法对数据进行加解密、签名/验签和密钥协商运算。应能支持给定密钥和明文（密文），检测其运算结果的正确性，包括：

a) 密码机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，解密结果和给定明文完全相同；
b) 密码机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，解密结果和给定明文完全相同；
c) 密码机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；
d) 密码机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；
e) 密码机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。

6.8.3 设备杂凑密码运算检测

服务器密码机应支持 SM3 算法。密码机可调用 SM3 算法对消息进行杂凑运算。应能支持对给定的消息和参数，调用 SM3 算法进行杂凑运算。

a) 密码机对给定消息调用 SM3 算法计算杂凑值，结果和给定杂凑值完全相同；
b) 密码机对给定消息和参数调用 SM3 算法计算杂凑值，结果和给定杂凑值完全相同。

6.9 设备随机数质量检测

服务器密码机应具备随机数生成功能，应至少具备 2 个独立的物理噪声源。随机数质量检测应遵循 GB/T 32915。

随机数检测程序由国家密码管理主管部门认可的检测机构设计提供。对服务器密码机进行随机数检测的检测结果应符合 GM/T 0005 要求。

服务器密码机采用的随机数发生器应能通过送样检测、出厂检测、上电检测和使用检测四个不同应用阶段的随机数检测：

a) 送样检测

依据 GM/T 0005 进行随机数检测。

b) 出厂检测

- 检测量：采集 $50*10^6$ 比特随机数，分成 50 组，每组 10^6 比特；
- 检测项目：依据 GM/T 0005 进行检测；
- 检测通过标准：检测中如果有一项不通过检测标准，则告警检测不合格；

允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

c) 上电检测

- 检测量：采集 $20*10^6$ 比特随机数，分成 20 组，每组 10^6 比特；
- 检测项目：依据 GM/T 0005 进行检测；
- 检测通过标准：检测中如果有一项不通过检测标准，则告警检测不合格。

允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

d) 使用检测

1) 周期检测

- 检测量：采集 $4*10^5$ 比特随机数，分成 20 组，每组 20000 比特；
- 检测项目：对采集随机数按照 GM/T 0005 中除离散傅立叶检测、线性复杂度检测、通用统计检测外的 12 项检测；
- 检测通过标准：检测中如果有一项不通过检测标准，则告警检测不合格。允许重复

1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效；

- 检测周期：可配置，检测间隔最长不超过 12h。

2) 单次检测

- 检测量：根据实际应用时每次所采随机数大小确定，但长度不应低于 128 比特，且已通过检测的未用序列可继续用；
- 检测项目：扑克检测。当样本长度小于 320 比特时，参数 m=2；
- 检测通过标准：检测中如果不通过检测标准，则告警检测不合格。

允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

6.10 设备应用接口检测

服务器密码机的应用编程接口应遵循 GM/T 0018。

服务器密码机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或调用过程，API 函数应返回相应的错误代码。密码机的 API 接口检测应包括以下 6 类：

a) 设备管理类函数；
b) 密钥管理类函数；
c) 对称算法运算类函数；
d) 非对称算法运算类函数；
e) 杂凑运算类函数；
f) 用户文件操作类函数。

6.11 设备远程管理接口检测

服务器密码机宜支持设备远程管理功能，若支持此功能，服务器密码机的设备远程管理接口应遵循 GM/T 0030。

服务器密码机宜能够通过设备远程管理接口实现参数配置、远程维护等功能，并且可通过设备远程管理接口查询设备信息库中的信息，对密码机进行监控和管理。包括设备状态查询、对设备告警信息的处理等。

服务器密码机将上层管理应用的管理请求转换为标准的消息调用，通过安全通道实现与管理应用间的消息传递。对于正确的调用环境或调用过程，设备管理类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或调用过程，设备远程管理类函数应返回相应的错误代码。密码机的远程管理接口检测应包括以下 11 类：

a) 初始化设备管理环境；
b) 退出设备管理环境；
c) 获取被管设备总数；
d) 根据设备号得到设备标识和信息；
e) 批量获取设备属性值；
f) 设置设备属性值；
g) 导出设备证书；
h) 发送数据；
i) 获得告警信息数量；
j) 获得一条告警信息；
k) 设置告警信息为已处理。

6.12 设备访问控制检测

服务器密码机应能够为内部存储的主体资源提供访问控制功能。登录服务器密码机应具备完善的身份认证机制，不同的管理操作应有不同的操作权限。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，破坏密码机的安全性。

对于存储在密码机内部的私钥，应持有正确的私钥访问控制码才能使用；对密码机功能的调用和对密码机的远程管理，应采用基于 IP 包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设备功能或对设备进行远程管理；不具备授权 IP 的主机不可正常调用设备功能或对设备进行远程管理。

6.13 设备日志记录检测

服务器密码机应提供日志记录、查看和导出功能。

服务器密码机的日志内容应包括：

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。

服务器密码机的日志内容宜包括：

a) 如与设备管理中心连接，则对相应操作进行记录；

b) 对应用接口中密钥管理相关调用记录日志。

6.14 设备性能检测

服务器密码机的各项密码运算应满足一定的性能指标。

密码机的性能检测应包括九方面：密码机随机数产生性能、密码机对称密钥产生性能、密码机非对称密钥产生性能、密码机 SM1 算法加解密性能、密码机 SM2 算法加解密性能、密码机 SM2 算法签名及验证性能、密码机 SM3 算法运算性能、密码机 SM4 算法加解密性能、密码机并发工作性能。密码机的每一项性能检测都应进行多次检测，结果取各次的平均值。

a) 密码机随机数产生性能检测：让服务器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，统计其完成时间 T（秒）。性能指标公式为：

$$S = 8LN/(1024 \times 1024T)$$；单位为 Mbps；

b) 密码机对称密钥产生性能检测：让服务器密码机生成并输出 M个密钥，测量其完成时间 T（秒）。性能指标公式为 $S = M/T$；单位为（组/秒）；

c) 密码机非对称密钥对产生性能检测：让服务器密码机生成并输出 M对密钥对，统计其完成时间 T（秒）。性能指标公式为 $S = M/T$；单位为（对/秒）；

d) 密码机 SM1 算法加解密性能检测：将一个长度为 L（字节）的数据报文，发送给服务器密码机进行加/解密操作，重复操作 N次，统计其完成时间 T（秒）。需分别测试 SM1 算法所支持的各种工作模式的性能，性能指标公式为：

$$S = 8LN/(1024 \times 1024T)$$；单位为 Mbps；

e) 密码机 SM2 算法加密/解密性能检测：将一个长度为 L 字节的数据报文，发送给服务器密码机进行加密/解密操作，重复操作 N次，测量其完成时间 T（秒）。性能指标公式为：

$$S = 8LN/(1024 \times 1024T)$$；单位为 Mbps；

f) 密码机 SM2 算法签名/验证性能检测：将一个定长的数据报文，发送给服务器密码机进行签名/验证操作，重复操作 N次，统计其完成时间 T（秒）。性能指标公式为：公式为 $S = N/T$；单位为（次/秒）；

g) 密码机 SM3 算法运算性能检测：将一个长度为 L（字节）的数据报文，发送给服务器密码机进行摘要运算，重复操作 N 次，测量其完成时间 T（秒）。性能指标公式为：

$$S = 8LN/(1024\times1024T)$$；单位为 Mbps；

h) 密码机 SM4 算法加解密性能检测：将一个长度为 L（字节）的数据报文，发送给服务器密码机进行加/解密操作，重复操作 N 次，测量其完成时间 T（秒）。需分别测试 SM4 算法所支持的各种工作模式的性能，性能指标公式为：

$$S = 8LN/(1024\times1024T)$$；单位为 Mbps；

i) 密码机并发工作性能检测：包括每秒新建连接数和最大并发连接数两个指标。

在检测平台模拟多个客户端行为，并行与服务器密码机建立 TCP 连接，重复此过程一段时间，取每秒建立连接数目的平均值作为每秒新建连接数测试结果，单位为条/秒。

在检测平台模拟多个客户端行为，并行与服务器密码机建立 TCP 连接，然后不断增加客户端，并重复此过程，直到无法建立并保持连接为止。取已经接入的 TCP 连接数目为测试结果，单位为条。

6.15 设备网络适应性检测

服务器密码机对使用主体的服务模式应该具备良好的适应性和扩展性，应满足至少三种模式的应用要求，包括：

a) 密码机应能够与主机直接连接使用；
b) 密码机应能够通过交换机同时与多台主机连接使用；
c) 密码机应能够与不同网段主机连接使用。

6.16 设备安全性检测

服务器密码机安全性检测遵照 GM/T0039。

6.17 设备环境适应性检测

服务器密码机设备环境适应性检测应达到 GM/T 0030-2014 第 6.3 节的要求。

6.18 设备可靠性检测

服务器密码机设备可靠性检测应达到 GM/T 0030-2014 第 6.4 节的要求。

7 送检文档技术要求

服务器密码机研制单位按照国家密码管理主管部门检测要求提交相关文档资料，作为服务器密码机的检测依据。文档资料应包含但不限于以下内容：

a) 密码机服务程序、应用编程接口和客户端管理软件的结构框图、流程图和基本功能的源代码；
b) 开机自检的工作原理说明；
c) 自测程序的工作原理说明；
d) 敏感数据信息的存储和使用说明；
e) 物理防护措施说明；
f) 技术工作总结报告；

g) 安全性设计报告；
h) 产品安装使用说明；
i) 密码算法自检原理说明文档；
j) 随机数自检原理说明文档。

附录 A
（资料性附录）
检测项目列表

A.1 设备外观及结构检查见表 A.1

表 A.1　设备外观及结构检测表

检测项目	检测子项目
设备外观及结构检测	应支持状态指示灯
	2 个 RJ45 网络接口
	支持冗余电源
	应支持电源指示灯
	1 个串口（RJ45 或 DB9）作为控制口
	手动密钥销毁开关
	1 个 DB9 串口
	USB 接口
	支持人机交互部件

A.2 设备状态检测项目见表 A.2

表 A.2　设备状态检测项目表

检测项目	检测子项目
设备状态检测	设备启动进入初始状态。
	初始化配置完成后，设备进入就绪状态。
	设备只能通过重新启动进入工作状态。
	设备唯一标识符查询
	设备状态包括硬件部件状态。
	设备状态包括软件状态。
	设备软件版本查询。
	设备硬件版本查询。

A.3 设备自检检测项目见表 A.3

表 A.3　设备自检检测项目表

检测项目	检测内容
设备自检检测	设备开机自动进行自检功能
	设备自检成功自动进入初始化配置或就绪工作状态
	设备自检失败报告检测结果并记录日志

A.4 设备配置管理检测项目见表 A.4

表 A.4　设备配置管理检测项目表

检测项目	检测内容

设备配置管理检测	设备具有配置管理权限控制功能
	设备可配置本地 IP 地址、掩码、端口
	设备可配置许可访问设备的主机 IP 地址
	设备可配置网关 IP 地址

A.5 设备密钥管理检测项目见表 A.5

表 A.5　设备密钥管理检测项目表

检测项目	检测子项目
设备密钥管理检测	设备可生成指定参数的非对称密钥对并存储在设备内部
	设备生成并存储的非对称密钥对的访问和使用可采用访问控制技术进行控制
	设备内部密钥可通过介质安全的备份
	设备内部密钥可通过备份介质安全的恢复
	设备内部密钥可通过备份介质安全的同步到相同的另一台设备
	设备内部存储的密钥对公钥可正常导出使用

A.6 设备 SM1 密码运算检测项目见表 A.6

表 A.6　设备 SM1 密码运算检测项目表

检测项目	检测内容
SM1 密码运算检测	给定密钥和明文 SM1 算法 ECB 模式加密
	给定密钥和密文 SM1 算法 ECB 模式解密
	给定密钥和明文 SM1 算法 CBC 模式加密
	给定密钥和密文 SM1 算法 CBC 模式解密
	给定密钥和明文 SM1 算法 OFB 模式加密
	给定密钥和密文 SM1 算法 OFB 模式解密
	给定密钥和明文 SM1 算法 CFB 模式加密
	给定密钥和密文 SM1 算法 CFB 模式解密

A.7 设备 SM2 密码运算检测项目见表 A.7

表 A.7　设备 SM2 密码运算检测项目表

检测项目	检测内容
SM2 密码运算检测	设备对给定的密钥和明文经 SM2 算法公钥加密，检测平台采用对应 SM2 算法私钥解密得到明文，解密结果和给定明文完全相同
	设备对给定的密钥和密文经 SM2 算法私钥解密，结果正确
	密码机对给定的密钥和明文经 SM2 算法签名，检测平台验证其签名，结果正确
	设备对给定的密钥和签名值经 SM2 算法验证签名，结果正确
	设备对给定的密钥和密钥协商参数经 SM2 算法产生会话密钥，结果正确

A.8 设备 SM3 密码运算检测项目见表 A.8

表 A.8　设备 SM3 密码运算检测项目表

检测项目	检测内容
SM3 密码运算检测	设备对给定的明文和参数经 SM3 算法计算杂凑值，结果正确

A.9 设备 SM4 密码运算检测项目见表 A.9

表 A.9　设备 SM4 密码运算检测项目表

检测项目	检测内容
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

A.10 设备随机数质量检测项目见表 A.10

表 A.10　设备随机数质量检测项目表

检测项目	检测内容
随机数检测	通过密码服务接口产生随机数，对随机数质量进行检测

A.11 设备应用接口检测项目见表 A.11

表 A.11　设备应用接口检测项目表

检测项目	检测内容
设备应用接口检测	设备管理类函数
	密钥管理类函数
	对称算法运算类函数
	非对称算法运算类函数
	杂凑运算类函数
	用户文件操作类函数

A.12 设备远程管理接口检测项目见表 A.12

表 A.12　设备远程管理接口检测项目表

检测项目	检测内容
设备远程管理接口检测	初始化设备管理环境
	退出设备管理环境
	获取被管设备总数

	根据设备号得到设备标识和信息
	批量获取设备属性值
	设置设备属性值
	导出设备证书
	发送数据
	获得一条告警信息
	设置告警信息为已处理
	设置设备属性值

A.13 设备访问控制检测项目见表 A.13

表 A.13　设备访问控制检测项目表

检测项目	检测内容
设备访问控制检测	无正确私钥访问控制码不能使用指定的设备内部私钥进行运算
	已许可 IP 的主机可正常调用设备功能
	未许可 IP 的主机不可正常调用设备功能

A.14 设备日志记录检测项目见表 A.14

表 A.14　设备日志记录检测项目表

检测项目	检测内容
设备日志记录检测	设备对管理员操作行为提供日志记录
	设备对异常事件提供日志记录
	设备日志可查看、可导出

A.15 设备性能检测项目见表 A.15

表 A.15　设备性能检测项目表

检测项目	检测内容
设备性能检测	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
	SM1 算法运算性能
	SM2 算法加解密性能
	SM2 算法签名验证性能
	SM3 算法运算性能
	SM4 算法运算性能
	设备并发工作性能

A.16 设备网络适应检测项目见表 A.16

表 A.16　设备网络适应检测项目表

检测项目	检测内容

设备网络适应检测	设备支持主机直接连接使用
	设备支持通过交换机同时与多台主机连接使用
	设备支持与不同网段主机连接使用

A.17 设备安全性检测项目见表 A.17

表 A.17　设备安全性检测项目表

检测项目	检测子项目
设备安全性检测	

A.18 设备环境适应性检测项目见表 A.18

表 A.18　设备环境适应性检测项目表

检测项目	检测子项目
设备环境适应性检测	

A.19 设备可靠性检测项目见表 A.19

表 A.19　设备环境适应性检测项目表

检测项目	**检测子项目**
设备可靠性检测	