

ICS 35.040
L 80
备案号:62994—2018



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

2018-05-02 发布

2018-05-02 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 检测环境要求	2
5.1 常规检测环境	2
5.2 跨网段检测环境	3
6 检测内容	3
6.1 概述	3
6.2 设备外观及结构检查	4
6.3 设备管理功能检查	4
6.4 设备状态检测	5
6.5 设备自检检测	5
6.6 设备配置管理检测	5
6.7 设备密钥管理检测	5
6.8 设备密码算法正确性与一致性检测	6
6.9 设备随机数质量检测	7
6.10 设备应用接口检测	8
6.11 设备远程管理接口检测	8
6.12 设备访问控制检测	8
6.13 设备日志记录检测	9
6.14 设备性能检测	9
6.15 设备网络适应性检测	10
6.16 设备安全性检测	10
6.17 设备环境适应性检测	10
6.18 设备可靠性检测	10
7 送检文档技术要求	10
附录 A (资料性附录) 检测项目列表	11

前 言

本标准按照 GB/T 1.1—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 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方法

GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法

GM/T 0005 随机数检测规范

GM/T 0018 密码设备应用接口规范

GM/T 0030—2014 服务器密码机技术规范

GM/T 0039 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。