ICS 35.040
L 80
备案号:58557—2017

GM

中华人民共和国密码行业标准

GM/T 0052—2016

密码设备管理
VPN设备监察管理规范

Cryptographic equipment management—
Monitoring management specification of VPN equipment

2016-12-23 发布　　2016-12-23 实施

国家密码管理局　　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

GM/T 0052《密码设备管理　VPN 设备监察管理规范》是密码设备管理类规范之一。该类规范由一个基础规范和系列管理应用规范组成，目前包括：

——基础规范：GM/T 0050　密码设备管理　设备管理技术规范；

——管理应用规范：GM/T 0051　密码设备管理　对称密钥管理规范；

——管理应用规范：GM/T 0052　密码设备管理　VPN 设备监察管理规范；

——管理应用规范：GM/T 0053　密码设备管理　远程监控与合规性检验接口数据规范。

本标准凡涉及密码算法相关内容，按国家有关法规实施。

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：上海信息安全工程技术研究中心、上海交通大学信息安全学院、上海鹏越惊虹信息技术发展有限公司、上海华堂网络有限公司、卫士通信息产业股份有限公司、上海天融信网络安全技术有限公司、上海信昊信息科技有限公司。

本标准主要起草人：王隽、田立、周志洪、黄志荣、廖烨、邹铷、袁峰、潘淑媛、王贺刚、李俊山、张元臣、吕明忠、潘利民、李高健。

引　言

本标准依据GM/T 0050《密码设备管理　设备管理技术规范》中密码设备管理平台架构，提出针对重要信息系统与网络中VPN设备的监察管理规范，包括管理体系、管理流程、管理消息格式等。本标准采用的安全通道，依据GM/T 0050中的管理应用接口建立，相关内容请参考GM/T 0050。

密码设备管理
VPN设备监察管理规范

1 范围

本标准规定了重要信息系统与网络中的VPN设备的监察管理，以发现和定位网络中的非法VPN设备，并检测合法设备在使用过程中的违规操作。

本标准适用于VPN设备监察管理系统及监察设备的研发与应用，也可用于指导检测该类监察设备。

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。

GM/T 0022—2014 IPSec VPN技术规范

GM/T 0024—2014 SSL VPN技术规范

GM/T 0050—2016 密码设备管理 设备管理技术规范

GM/T 0053—2016 密码设备管理 远程监控与合规性检验接口数据规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

VPN设备 VPN device

利用VPN技术实现网络中安全通信服务的设备。本标准中的VPN设备指IPsec VPN和SSL VPN设备，包括采用IPsec、SSL协议的符合国家标准的网络密码机。

3.2

VPN设备的监察设备 VPN compliance monitoring agency

按照监察管理应用规则，实现对被监测网络中的目的数据包进行过滤分析，并上报关键信息的网络设备。

3.3

伯克利封包过滤器 berkeley packet filter

工作在操作系统内核的数据包捕获机制，先将链路层的数据包捕获再过滤，最后提供给应用层特定的过滤后的数据包。

3.4

白名单 white list

对已在国家密码管理主管部门备过案，并且“已知为良好”的VPN设备名单，管理应用层用来标识安全可信的合规设备列表。白名单中的信息包括：设备的注册IP地址、设备的密码算法标识等信息。