ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 32922—2023
代替 GB/T 32922—2016

信息安全技术　IPSec VPN 安全接入基本要求与实施指南

Information security technology—Baseline and implementation guide of IPSec VPN securing access

2023-03-17 发布　　2023-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件代替GB/T 32922—2016《信息安全技术　IPSec VPN安全接入基本要求与实施指南》，与GB/T 32922—2016相比，除结构调整和编辑性改动外，主要技术变化如下：

——增加了IPSec VPN安全接入点到多点场景（见5.1.2）；

——更改了IPSec VPN安全接入场景的示意图（见第5章，2016年版的第5章）；

——更改了IPSec VPN网关密码算法的使用要求（见6.1.1，2016年版的6.1.1）；

——更改了IPSec VPN网关VPN功能要求的描述（见6.1.2，2016年版的6.1.2）；

——更改了IPSec VPN网关可靠性功能要求的描述（见6.1.2，2016年版的6.1.2）；

——增加了IPSec VPN网关在分支多出口场景支持动态选路功能的描述（见6.1.2）；

——更改了IPSec VPN网关互通兼容性功能要求的描述（见6.1.2，2016年版的6.1.2）；

——更改了IPSec VPN网关IPv6兼容性功能要求的描述（见6.1.2，2016年版的6.1.2）；

——增加了IPSec VPN网关易用性功能要求的描述（见6.1.2）；

——更改了IPSec VPN网关证书认证功能要求的描述（见6.1.2，2016年版的6.1.2）；

——更改了IPSec VPN网关产品的性能要求（见6.1.3，2016年版的6.1.3）；

——更改了IPSec VPN客户端技术要求，合并软硬件要求子章节（见6.2，2016年版的6.2）；

——更改了IPSec VPN网关和客户端功能要求中IPSec安全协议类型的要求（见6.1.2和6.2，2016年版的6.1.2和6.2）；

——更改了IPSec VPN网关及客户端设备管理要求（见6.3.1，2016年版的6.3.1）；

——更改了IPSec VPN网关和客户端证书管理要求的描述（见6.3.2，2016年版的6.3.2）；

——增加了“密码要求”（见6.4）；

——更改了实施指南相关描述（见第7章，2016年版的第7章）；

——更改了典型应用场景的描述（见附录A，2016年版的附录A）；

——增加了“常见的IPSec VPN功能”附录（见附录B），并调整原附录B为附录C；

——删除了传输模式IPSec 6over4隧道场景（见2016年版的附录C.2）。

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。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：国家信息中心、华为技术有限公司、奇安信网神信息技术（北京）股份有限公司、北京天融信网络安全技术有限公司、深信服科技股份有限公司、成都卫士通信息产业股份有限公司、深圳奥联信息安全技术有限公司、深圳市数元信安科技有限公司、中国科学院信息工程研究所、公安部第一研究所、新华三技术有限公司、西安交大捷普网络科技有限公司、鼎铉商用密码测评技术（深圳）有限公司、中国电力科学研究院有限公司。

本文件主要起草人：徐春学、焦迪、罗海宁、潘伟、王伟、曹金、李金国、万志宇、程子栋、王鹏彪、赵国全、罗俊、但波、翟鹏、任飞、田之洋、何建锋、万晓兰、姜敏、邹超、刘松、李海涛。

本文件及其所代替文件的历次版本发布情况为：

——2016年首次发布为GB/T 32922—2016；

——本次为第一次修订。

信息安全技术　IPSec VPN 安全接入基本要求与实施指南

1　范围

本文件规定了 IPSec VPN 安全接入应用过程中网关、客户端、安全管理以及密码应用等方面的基本要求，提供了采用 IPSec VPN 技术实现安全接入的典型场景和实施过程指南。

本文件适用于采用 IPSec VPN 技术开展安全接入应用的机构，指导其基于 IPSec VPN 技术开展安全接入平台或系统的需求分析、方案设计、方案验证、配置实施、运行管理。

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 15843（所有部分）　信息技术　安全技术　实体鉴别

GB/T 19713　信息技术　安全技术　公钥基础设施　在线证书状态协议

GB/T 20518　信息安全技术　公钥基础设施　数字证书格式

GB/T 25069　信息安全技术　术语

GB/T 32915　信息安全技术　二元序列随机性检测方法

GB/T 36968　信息安全技术　IPSec VPN 技术规范

GB/T 37092　信息安全技术　密码模块安全要求

GB/T 38636　信息安全技术　传输层密码协议（TLCP）

GM/T 0023　IPSec VPN 网关产品规范

GM/T 0050　密码设备管理　设备管理技术规范

GM/T 0062　密码产品随机数检测要求

GM/T 0089　简单证书注册协议规范

3　术语和定义

GB/T 25069、GB/T 36968 界定的以及下列术语和定义适用于本文件。

3.1

IPSec 协议　Internet Protocol Security

一种开放标准的框架结构，通过使用加密的安全服务以确保在公开网络上进行保密而安全的通信，可在端至端的层面上提供数据完整性保护、数据源鉴别、载荷机密性和抗重放攻击等安全服务。

［来源：GB/T 36968—2018，3.4，有修改］

3.2

虚拟专用网　virtual private network

使用密码技术在通信网络中构建安全通道的技术。

［来源：GB/T 36968—2018，3.7］