ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36968—2018

信息安全技术　IPSec VPN 技术规范

Information security technology—Technical specification for IPSec VPN

2018-12-28 发布　　2019-07-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:无锡江南信息安全工程技术中心、国家密码管理局商用密码检测中心、上海格尔软件股份有限公司、北京数字认证股份有限公司、山东得安信息技术有限公司、北京天融信网络安全技术有限公司、华为技术有限公司、深信服科技股份有限公司、深圳奥联信息安全技术有限公司、成都卫士通信息产业股份有限公司、北京三未信安科技发展有限公司。

本标准主要起草人:刘平、徐文耀、周国良、郑强、李述胜、马洪富、罗鹏、李金国、王雨晨、林国强、但波、罗俊、许永欣。

信息安全技术　IPSec VPN 技术规范

1　范围

本标准规定了 IPSec VPN 的技术协议、产品要求和检测方法。

本标准适用于 IPSec VPN 产品的研制、检测、使用和管理。

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 20518　信息安全技术　公钥基础设施　数字证书格式

GB/T 25056　信息安全技术　证书认证系统密码及其相关安全技术规范

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方法

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 35276　信息安全技术　SM2 密码算法使用规范

RFC 2408　互联网安全联盟和密钥管理协议(Internet Security Association and Key Management Protocol)

RFC 3947　密钥交换过程中 NAT 穿越协商(Negotiation of NAT-Traversal in the IKE)

RFC 3948　IPSec ESP 包的 UDP 封装(UDP Encapsulation of IPsec ESP Packets)

3　术语和定义

下列术语和定义适用于本文件。

3.1

安全联盟　security association

两个通信实体经协商建立起来的一种协定，它描述了实体如何利用安全服务来进行安全的通信。

注：安全联盟包括了执行各种网络安全服务所需要的所有信息，例如 IP 层服务(如头鉴别和载荷封装)、传输层和应用层服务或者协商通信的自我保护。

3.2

互联网安全联盟和密钥管理协议　internet security association and key management protocol

一个在互联网环境中建立安全联盟和进行密钥管理的协议。它定义了建立、协商、修改和删除安全联盟的过程和报文格式，以及交换密钥产生和鉴别数据的载荷格式。这些格式为传输密钥和鉴别信息提供了一致的框架。

3.3

载荷　payload

ISAKMP 通信双方交换消息的数据格式，是构造 ISAKMP 消息的基本单位。