ICS 35.040
L 80

中华人民共和国国家标准

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

2016-08-29 发布　　2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
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。

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:国家信息中心、华为技术有限公司、中安网脉(北京)技术股份有限公司、网神信息技术(北京)股份有限公司、北京天融信科技股份有限公司、迈普通信技术股份有限公司。

本标准主要起草人:罗海宁、周民、吕品、冷默、黄敏、徐浩、张锐卿、任献永、徐惠清、邵国安。

引　言

本标准主要内容包括 IPSec VPN 安全接入基本要求和基于 IPSec VPN 技术建设安全接入平台或系统的实施指南，其中“基本要求”对 IPSec VPN 安全接入应用过程中有关网关、客户端以及安全管理方面提出技术要求，“实施指南”主要适用于采用 IPSec VPN 技术开展安全接入应用的机构，指导其进行基于 IPSec VPN 技术的安全接入平台或系统的需求分析、方案设计、配置实施、测试与备案、运行管理。同时，本标准也可为相关设备厂商进行产品的设计和开发提供参考。

本标准是在国家电子政务外网 IPSec VPN 安全接入应用实践基础上归纳总结并提出的技术标准，也可广泛适用于 IPSec VPN 各种应用场景。

信息安全技术　IPSec VPN 安全接入基本要求与实施指南

1　范围

本标准明确了采用 IPSec VPN 技术实现安全接入的场景，提出了 IPSec VPN 安全接入应用过程中有关网关、客户端以及安全管理等方面的要求，同时给出了 IPSec VPN 安全接入的实施过程指导。

本标准适用于采用 IPSec VPN 技术开展安全接入应用的机构，指导其进行基于 IPSec VPN 技术开展安全接入平台或系统的需求分析、方案设计、配置实施、测试与备案、运行管理，也适用于设备厂商参考其进行产品的设计和开发。

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 20518—2006　信息安全技术　公钥基础设施　数字证书格式

GB/T 25069—2010　信息安全技术　术语

GM/T 0003—2012(所有部分)　SM2 椭圆曲线公钥密码算法

GM/T 0004—2012　SM3 密码杂凑算法

GM/T 0016—2012　智能密码钥匙密码应用接口规范

GM/T 0017—2012　智能密码钥匙密码应用接口数据格式规范

GM/T 0022—2014　IPSec VPN 技术规范

GM/T 0023—2014　IPSec VPN 网关产品规范

3　术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

第二层隧道协议　layer 2 tunneling protocol

L2TP

一种支持 VPN 的隧道协议，本身不提供加密功能。

3.2

IP 安全协议　IP security

IPSec

一套用于保护 IP 通信的安全协议，是 IPv4 的一个可选协议系列，也是 IPv6 的组成部分之一。

3.3

虚拟专用网　virtual private network

VPN

一种在公共通信基础网络上通过逻辑方式隔离出来的网络。