ICS 35.040
L 80
备案号:44623—2014

GM

中华人民共和国密码行业标准

GM/T 0022—2014

IPSec VPN 技术规范

IPSec VPN specification

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　发 布

目　　次

前　言

本标准依据 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：无锡江南信息安全工程技术中心、华为技术有限公司、深圳市奥联科技有限公司、深圳市深信服电子科技有限公司、山东得安信息技术有限公司、北京数字认证股份有限公司、上海格尔软件股份有限公司、武汉三江航天网络通信有限公司、西安交大捷普网络科技有限公司、北京天融信网络安全技术有限公司、迈普通信技术股份有限公司、国家密码管理局商用密码检测中心、杭州奕锐电子有限公司。

本标准主要起草人：刘平、朱志强、董浩、雷建、刘建锋、李小京、邱钢、向明、孔凡玉、李述胜、谭武征、王振、张勇、潘利民、范恒英、罗鹏、李渝川。

IPSec VPN 技术规范

1 范围

本标准对 IPSec VPN 的技术协议、产品管理和检测进行了规定，可用于指导 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。

GM/T 0005 随机性检测规范

GM/T 0009 SM2 密码算法使用规范

GM/T 0014 数字证书认证系统密码协议规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

RFC 3948 UDP Encapsulation of IPSec ESP Packets January 2005

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

密码算法 cryptographic algorithm

描述密码处理过程的运算规则。

3.1.2

密码杂凑算法 cryptographic hash algorithm

又称杂凑算法、密码散列算法或哈希算法。该算法将一个任意长的比特串映射到一个固定长的比特串，且满足下列三个特性：

a) 为一个给定的输出找出能映射到该输出的一个输入是计算上困难的；

b) 为一个给定的输入找出能映射到同一个输出的另一个输入是计算上困难的；

c) 要发现不同的输入映射到同一输出是计算上困难的。

3.1.3

非对称密码算法/公钥密码算法 asymmetric cryptographic algorithm/public key cryptographic algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥(公钥)可以公开，另一个密钥(私钥)必须保密，且由公钥求解私钥是计算不可行的。

3.1.4

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。