ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0022—2023
代替 GM/T 0022—2014

IPSec VPN 技术规范

IPSec VPN technical specification

2023-12-04 发布　　2024-06-01 实施

国家密码管理局　　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GM/T 0022—2014《IPSec VPN技术规范》，与GM/T 0022—2014相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 删除了术语和定义："密码算法"（见2014年版的3.1.1）、"密码杂凑算法"（见2014年版的3.1.2）、"非对称密码算法/公钥密码算法"（见2014年版的3.1.3）、"对称密码算法"（见2014年版的3.1.4）、"分组密码算法"（见2014年版的3.1.5）、"密码分组链接工作模式"（见2014年版的3.1.6）、"初始化向量/值"（见2014年版的3.1.7）、"数字证书"（见2014年版的3.1.9）、"鉴别"（见2014年版的3.1.14）、"加密"（见2014年版的3.1.15）、"SM1算法"（见2014年版的3.1.20）、"SM2算法"（见2014年版的3.1.21）、"SM3算法"（见2014年版的3.1.22）、"SM4算法"（见2014年版的3.1.23）；

b) 增加了术语和定义"可鉴别的加密机制"（见3.6）；

c) 增加了"缩略语"GCM和PRF（见4.2）；

d) 增加了与GCM加密模式相关的加密密钥选取说明（见6.1.3.3）；

e) 更改了与GCM加密模式相关的快速模式中消息1的数据包格式（见6.1.6.8，2014年版的5.1.5.7）、快速模式中消息2的数据包格式（见6.1.6.9，2014年版的5.1.5.8）、快速模式中消息3的数据包格式（见6.1.6.10，2014年版的5.1.5.9）；

f) 更改了"封装安全载荷ESP头格式"中与GCM相关的数据包封装和解封操作的详细说明（见6.2.2.2，2014年版的5.2.2.2）、"封装安全载荷ESP的处理"中与GCM相关的数据包封装和解封操作的详细说明（见6.2.2.3，2014年版的5.2.2.3）；

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。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：深信服科技股份有限公司、无锡江南计算技术研究所、格尔软件股份有限公司、迈普通信技术股份有限公司、北京数字认证股份有限公司、华为技术有限公司、中电科网络安全科技股份有限公司、西安交大捷普网络科技有限公司、山东得安信息技术有限公司、国家密码管理局商用密码检测中心、深圳奥联信息安全技术有限公司、中国科学院信息工程研究所、鼎铉商用密码测评技术（深圳）有限公司、北京天融信网络安全技术有限公司、奇安信网神信息技术（北京）股份有限公司、武汉三江航天网络通信有限公司、中国电子技术标准化研究院、深圳市网安计算机安全检测技术有限公司、杭州奕锐电子有限公司、智巡密码（上海）检测技术有限公司。

本文件主要起草人：刘平、叶润国、罗俊、郑强、付夏冰、范恒英、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、罗鹏、李渝川、徐明翼、马洪富、凌杭、周欣、王雨晨、何建锋、李琳、龙军、刘松、但波、雷晓锋、刘玉岭、燕爽、王银平、吴安然、安高峰、刘晨、赵松、曹金、李露、樊俊诚、黄敏、吴俊雄、顾伟平、杨柳、匡云。

本文件及其所代替文件的历次版本发布情况为：

——2014年首次发布为GM/T 0022—2014；

——本次为第一次修订。

IPSec VPN 技术规范

1 范围

本文件规定了 IPSec VPN 的技术协议和产品功能，包括密钥交换协议和安全报文协议，以及产品功能要求和安全管理要求。

本文件适用于 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 20518—2018 信息安全技术 公钥基础设施 数字证书格式

GB/T 32905—2016 信息安全技术 SM3 密码杂凑算法

GB/T 32907—2016 信息安全技术 SM4 分组密码算法

GB/T 35276—2017 信息安全技术 SM2 密码算法使用规范

GB/T 36624—2018 信息技术 安全技术 可鉴别的加密机制

GM/T 0005—2021 随机性检测规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0062—2018 密码产品随机数检测要求

GM/T 0092—2020 基于 SM2 算法的证书申请语法规范

GM/Z 4001 密码术语

RFC 2408 互联网安全联盟与密钥管理协议（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）

RFC 4304 互联网安全关联和密钥管理协议（ISAKMP）IPsec 解释域（DOI）的扩展序列号（ESN）附录［Extended sequence number （ESN） addendum to IPsec domain of interpretation （DOI） for ISAKMP］

3 术语和定义

GM/Z 4001 界定的以及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。

注 1：它描述了实体如何利用安全服务来进行安全的通信。

注 2：安全联盟包括了执行各种网络安全服务所要求的所有信息，例如：IP 层服务（如头鉴别和载荷封装）、传输层