

ICS 33.040.40

M 32

YD

中华人民共和国通信行业标准

YD/T 1897-2009

互联网密钥交换协议（IKEv2）技术要求

Technical requirements of Internet Key Exchange Protocol (IKEv2)

2009-06-15 发布

2009-09-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
4 IKE 基本使用与操作	2
5 IKE 协议细节及变化	8
6 报头和载荷的格式	23
7 一致性要求	48
8 安全性考虑	49
附录 A (资料性附录) 与 IKE 版本 1 的区别汇总	51
附录 B (资料性附录) Diffie-Hellman 组	52
参考文献	53

前 言

本标准是 IP 安全协议 (IPSec) 系列标准之一, 该系列标准的名称及结构预计如下:

1. 《IP 安全协议体系结构》(MOD IETF RFC2401)
2. 《IP 认证头(AH)》(MOD IETF RFC2402)
3. 《IP 封装安全载荷(ESP)》(MOD IETF RFC2406)
4. YD/T 1466-2006 《IP 安全协议 (IPSec) 技术要求》
5. YD/T 1467-2006 《IP 安全协议 (IPSec) 测试方法》
6. 《IP 安全协议 (IPSec) 穿越网络地址翻译 (NAT) 技术要求》
7. 《互联网密钥交换协议 (IKEv2) 技术要求》
8. 《互联网密钥交换协议 (IKEv2) 测试方法》

本标准与《互联网密钥交换协议 (IKEv2) 测试方法》配套使用。

本标准的附录 A、附录 B 均为资料性附录。

本标准由中国通信标准化协会提出并归口。

本标准起草单位: 工业和信息化部电信研究院

本标准起草人: 谢 玮、刘 述、田慧蓉、马 科、马军峰、高 巍、江浩洁、唐 浩、武 静、
吴英桦