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。

3.1.5

分组密码算法　block cipher algorithm

将输入数据划分成固定长度的分组进行加解密的一类对称密码算法。

3.1.6

密码分组链接工作模式　cipher block chaining operation mode;CBC

分组密码算法的一种工作模式，其特征是将当前的明文分组与前一密文分组进行异或运算后再进行加密得到当前的密文分组。

3.1.7

初始化向量/值　initialization vector/initialization value;IV

在密码变换中，为增加安全性或使密码设备同步而引入的用于数据变换的起始数据。

3.1.8

数据源鉴别　data origin authentication

确认接收到的数据的来源是所声称的。

3.1.9

数字证书　digital certificate

也称公钥证书，由证书认证机构(CA)签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.1.10

安全联盟　security association;SA

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。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。

3.1.11

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

互联网安全联盟和密钥管理协议定义了建立、协商、修改和删除安全联盟的过程和报文格式，并定义了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。

3.1.12

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。

3.1.13

IPSec协议　Internet Protocol Security

由IETF制定的端到端的确保基于IP通信数据安全性的一种网络层协议，可以提供数据完整性保护、数据源鉴别、载荷机密性和抗重放攻击等安全服务。

3.1.14

鉴别　authentication

鉴别机制使IP通信的数据接收方能够确认数据发送方的真实身份以及数据在传输过程中是否遭到篡改。

3.1.15

加密　encipherment/encryption

对数据进行密码变换以产生密文的过程。

3.1.16

鉴别头　authentication header；AH

属于 IPSec 的一种协议，用于提供 IP 数据包的数据完整性、数据源鉴别以及抗重放攻击的功能，但不提供数据机密性的功能。

3.1.17

封装安全载荷　encapsulating security payload；ESP

属于 IPSec 的一种协议，用于提供 IP 数据包的机密性、数据完整性以及对数据源鉴别以及抗重放攻击的功能。

3.1.18

虚拟专用网络　virtual private network；VPN

使用密码技术在通信网络中构建安全通道的技术。

3.1.19

IPSec 实现　IPSec implementation

具体实现 IPSec VPN 协议的软硬件产品。

3.1.20

SM1 算法　SM1 algorithm

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

3.1.21

SM2 算法　SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为 256 比特。

3.1.22

SM3 算法　SM3 algorithm

一种密码杂凑算法，其输出为 256 比特。

3.1.23

SM4 算法　SM4 algorithm

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

3.2　缩略语

下列缩略语适用于本文件。

AH：鉴别头(Authentication Header)

CBC ：(分组密码的)密码分组链接(工作方式)(Cipher Block Chaining)

ESP：封装安全载荷(Encapsulating Security Payload)

HMAC：带密钥的杂凑运算(Keyed-Hash Message Authentication Code)

IPSec：IP 安全协议(Internet Protocol Security)

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

IV：初始化向量(Initialization Vector)

NAT：网络地址转换(Network Address Translation)

SA：安全联盟(Security Association)

VPN：虚拟专用网络(Virtual Private Network)

4 密码算法和密钥种类

4.1 密码算法

IPSec VPN 使用国家密码管理主管部门批准的非对称密码算法、对称密码算法、密码杂凑算法和随机数生成算法。算法及使用方法如下：

——非对称密码算法使用 SM2 椭圆曲线密码算法，也可支持 2048 位及以上的 RSA 算法，用于实体验证、数字签名和数字信封等。

——对称密码算法使用 SM1 或 SM4 分组密码算法，用于密钥交换数据的加密保护和报文数据的加密保护。算法的工作模式使用 CBC 模式。

——密码杂凑算法使用 SM3 或 SHA-1 密码杂凑算法，用于完整性校验。

——随机数生成算法生成的随机数应能通过 GM/T 0005 规定的检测。

4.2 密钥种类

IPSec VPN 使用下列密钥：

——设备密钥：非对称算法使用的公私钥对，包括签名密钥对和加密密钥对，用于实体验证、数字签名和数字信封等。

——工作密钥：在密钥交换第一阶段得到的密钥，用于会话密钥交换过程的保护。

——会话密钥：在密钥交换第二阶段得到的密钥，用于数据报文及报文 MAC 的加密。

5 协议

5.1 密钥交换协议

密钥交换协议定义了协商、建立、修改、删除安全联盟的过程和报文格式。协议报文使用 UDP 协议 500 端口进行传输。

本章用到的符号如下：

HDR：一个 ISAKMP 头。

HDR * ：表示 ISAKMP 头后面的载荷是加密的。

SA：带有一个或多个建议载荷的安全联盟载荷。

IDi：发起方的标识载荷。

IDr：响应方的标识载荷。

HASHi：发起方的杂凑载荷。

HASHr：响应方的杂凑载荷。

SIGi：发起方的签名载荷。

SIGr：响应方的签名载荷。

CERT_sig_r：签名证书载荷。

CERT_enc_r：加密证书载荷。

Ni：发起方的 nonce 载荷。

Nr：响应方的 nonce 载荷。

<p>_b：载荷<p>的主体，就是没有 ISAKMP 通用头的载荷。

pub_i：发起方公钥。

pub_r：响应方公钥。

prv_i:发起方私钥。

prv_r:响应方私钥。

CKY-I:ISAKMP 头中的发起方 cookie。

CKY-R:ISAKMP 头中的响应方 cookie。

x | y:x 与 y 串接。

[x]:x 为可选。

Asymmetric_Encrypt(msg, pub_key):使用非对称算法 Asymmetric,pub_key 作为密钥对输入信息 msg_b 进行加密,其输出为 msg 的通用载荷头和密文串接。如 RSA_Encrypt(Ski, pub_key)表示使用 RSA 算法,使用公钥 pub_key 对 Ski_b 进行加密,其输出为 Ski 的通用载荷头和密文串接。

Asymmetric_Sign (msg, priv_key):使用非对称算法 Asymmetric,priv_key 作为密钥对 msg 进行数字签名。

Symmetric_Encrypt(msg,key):使用对称算法 Symmetric,key 作为密钥对输入信息 msg_b 进行加密,其输出为 msg 的通用载荷头和密文串接。如 SM1_Encrypt (Ni, key)表示使用 SM1 算法,使用 key 作为密钥对 Ni_b 进行加密,其输出为 Ni 的通用载荷头和密文串接。

HASH(msg):使用密码杂凑算法对 msg 进行数据摘要运算。

PRF(key,msg):使用密钥 key 对消息 msg 进行数据摘要运算。

5.1.1 交换阶段及模式

5.1.1.1 交换阶段

密钥交换协议包括第一阶段和第二阶段。

在第一阶段交换中,通信双方建立了一个 ISAKMP SA。该 SA 是协商双方为保护它们之间的通信而使用的共享策略和密钥。用这个 SA 来保护 IPSec SA 的协商过程。一个 ISAKMP SA 可以用于建立多个 IPSec SA。

在第二阶段交换中,通信双方使用第一阶段 ISAKMP SA 协商建立 IPSec SA,IPSec SA 是为保护它们之间的数据通信而使用的共享策略和密钥。

5.1.1.2 交换模式

本标准规定了两种交换模式,分别为主模式和快速模式。

主模式用于第一阶段交换,实现通信双方的身份鉴别和密钥交换,得到工作密钥,该工作密钥用于保护第二阶段的协商过程。

快速模式用于第二阶段交换,实现通信双方 IPSec SA 的协商,确定通信双方的 IPSec 安全策略及会话密钥。

5.1.2 交换

交换使用标准 ISAKMP 载荷语法、属性编码、消息的超时和重传以及通知消息。

安全联盟 SA 采用的载荷封装形式为:变换载荷封装在建议载荷中,建议载荷封装在安全联盟载荷中。本标准不限制发起方可以发给响应方的提议数量,如果第一阶段交换中有多个变换载荷,应将多个变换载荷封装在一个建议载荷中,然后再将它们封装在一个安全联盟载荷中。安全联盟的定义参见附录 A,有关变换载荷、建议载荷、安全联盟载荷等的具体定义见 5.1.4。

在安全联盟的协商期间,响应方不能修改发起方发送的任何提议的属性。否则,交换的发起方应终止协商。

5.1.2.1 第一阶段——主模式

主模式是一个身份保护的交换，其交换过程由 6 个消息组成。双方身份的鉴别采用数字证书的方式。

本阶段涉及的消息头及载荷的具体内容见 5.1.4。

主模式的交换过程如下：

消息序列	发起方 i	方向	响应方 R
1	HDR, SA	—>	
2		<—	HDR, SA,CERT_sig_r,CERT_enc_r
3	HDR, XCHi, SIGi	—>	
4		<—	HDR, XCHr, SIGr
5	HDR*, HASHi	—>	
6		<—	HDR*, HASHr

消息 1　发起方向响应方发送一个封装有建议载荷的安全联盟载荷，而建议载荷中又封装有变换载荷。

消息 2　响应方发送一个安全联盟载荷以及响应方的签名证书和加密证书，该载荷表明它所接受的发起方发送的 SA 提议。安全联盟载荷的具体内容见 5.1.4.3。

消息 3 和消息 4　发起方和响应方交换数据，交换的数据内容包括 nonce、身份标识(ID)等载荷。Nonce 是生成加密密钥和认证密钥所必需的参数；ID 是发起方或响应方的标识。这些数据使用临时密钥 Sk 进行加密保护，Sk 用对方加密证书中的公钥加密保护，并且，双方各自对数据进行数字签名。当使用 SM2 算法进行加密和数字签名时，参见 GM/T 0009；当使用 RSA 算法进行加密和数字签名时，见 PKCS#1。

发起方交换的数据如下：

XCHi = Asymmetric_Encrypt(Ski, pub_r) | Symmetric_Encrypt(Ni,Ski) | Symmetric_Encrypt(IDi,Ski)|CERT_sig_i|CERT_enc_i

SIGi_b = Asymmetric_Sign(Ski_b | Ni_b | IDi_b | CERT_enc_i_b, priv_i)

响应方交换的数据如下：

XCHr = Asymmetric_Encrypt(Skr, pub_i) | Symmetric_Encrypt(Nr, Skr) | Symmetric_Encrypt(IDr,Skr)

SIGr_b = Asymmetric_Sign(Skr_b | Nr_b | IDr_b|CERT_enc_r_b, priv_r)

上述过程中使用的非对称密码算法、对称密码算法和密码杂凑算法均由消息 1 和消息 2 确定。临时密钥 Sk 由发起方和响应方各自随机生成，其长度应符合对称密码算法对密钥长度的要求。

对称密码运算使用 CBC 模式，第一个载荷的 IV 值为 0；后续的 IV 使用前面载荷的最后一组密文。

加密前的交换数据应进行填充，使其长度等于对称密码算法分组长度的整数倍。所有的填充字节的值除最后一个字节外都是 0，最后一个填充字节的值为不包括它自己的填充字节数。

Idi 和 Idr 的类型应使用 ID_DER_ASN1_DN。

如果对方证书已经在撤销列表中，系统应发送 INVALID_CERTIFICATE 通知消息。

消息 3 和消息 4 交互完成后，参与通信的双方生成基本密钥参数 SKEYID，以生成后续密钥 SKEYID_d、SKEYID_a、SKEYID_e，计算方法分别如下：

SKEYID = PRF(HASH(Ni_b | Nr_b), CKY-I | CKY-R)

SKEYID_d = PRF(SKEYID, CKY-I | CKY-R | 0)

SKEYID_a = PRF(SKEYID, SKEYID_d | CKY-I | CKY-R | 1)

SKEYID_e = PRF(SKEYID, SKEYID_a | CKY-I | CKY-R | 2)

上述计算公式中的值0,1,2是单个字节的数值。

SKEYID_e是ISAKMP SA用来保护其消息机密性所使用的工作密钥。SKEYID_a是ISAKMP SA用来验证其消息完整性以及数据源身份所使用的工作密钥。SKEYID_d用于会话密钥的产生。

所有SKEYID的长度都由PRF函数的输出长度决定。如果PRF函数的输出长度太短,不能作为一个密钥来使用,则SKEYID_e应进行扩展。例如,HMAC HASH的一个PRF可产生128比特的输出,但密码算法要求用到大于128比特的密钥的时候,SKEYID_e就需要利用反馈及连接方法加以扩展,直到满足对密钥长度的要求为止。反馈及连接方法如下:

K = K1 | K2 | K3…

K1 = PRF(SKEYID_e, 0)

K2 = PRF(SKEYID_e, K1)

K3 = PRF(SKEYID_e, K2)

…

最后从K的起始位置开始取密码算法的密钥所需要的位数。

消息5和消息6　发起方和响应方鉴别前面的交换过程。这两个消息中传递的信息使用对称密码算法加密。对称密码算法由消息1和消息2确定,密钥使用SKEYID_e。对称密码运算使用CBC模式,初始化向量IV是消息3中的Ski和消息4中的Skr串连起来经过HASH运算得到的,即:

IV= HASH(Ski_b | Skr_b)

Hash算法由消息1和消息2确定。

加密前的消息应进行填充,使其长度等于对称密码算法分组长度的整数倍。所有的填充字节的值都是0。报头中的消息长度应包括填充字节的长度,因为这反映了密文的长度。

为了鉴别交换,发起方产生HASH_I,响应方产生HASH_R,计算公式如下:

HASH_I = PRF(SKEYID, CKY-I | CKY-R | SAi_b | IDi_b)

HASH_R = PRF(SKEYID, CKY-R | CKY-I | SAr_b | IDr_b)

5.1.2.2　第二阶段——快速模式

快速模式交换依赖于第一阶段主模式交换,作为IPSec SA协商过程的一部分协商IPSec SA的安全策略并衍生会话密钥。快速模式交换的信息由ISAKMP SA来保护,即除了ISAKMP头外所有的载荷都要加密。在快速模式中,一个HASH载荷应紧跟在ISAKMP头之后,这个HASH用于消息的完整性校验以及数据源身份验证。

在第二阶段,载荷的加密使用对称密码算法的CBC工作模式,第1个消息的IV是第一阶段的最后一组密文和第二阶段的MsgID进行HASH运算所得到的,即:

IV=HASH(第一阶段的最后一组密文 | MsgID)

后续的IV是前一个消息的最后一组密文。消息的填充和第一阶段中的填充方式一样。

在ISAKMP头中的MsgID唯一标识了一个正在进行中的快速模式,而该ISAKMP SA本身又由ISAKMP头中的cookies来标识。因为快速模式的每个实例使用一个唯一的IV,这就有可能基于一个ISAKMP SA的多个快速模式在任一时间内同时进行。

在快速模式协商中,身份标识ID缺省定义为ISAKMP双方的IP地址,并且没有强制规定允许的协议或端口号。如果协商双方需要指定ID,则双方的身份应作为IDi和IDr被依次传递。响应方的本地安全策略将决定是否接受对方的身份标识ID。如果发起方的身份标识ID由于安全策略或其他原因没有被响应方所接受,则响应方应该发送一个通知消息类型为INVALID_ID_INFORMATION (18)的通知载荷。

在通信双方之间有多条隧道同时存在的情况下,身份标识ID为对应的IPSec SA标识并规定通信数据流进入对应的隧道。

本阶段涉及的消息头及载荷的具体内容见 5.1.4。

快速模式的交换过程如下：

消息序列	发起方	方向	响应方
1	HDR*，HASH(1)，SA，Ni[，IDci，IDcr]	—>	
2		<—	HDR*，HASH(2)，SA，Nr[，IDci，IDcr]
3	HDR*，HASH(3)	—>	

消息 1　发起方向响应方发送一个杂凑载荷、一个安全联盟载荷(其中封装了一个或多个建议载荷，而每个建议载荷中又封装一个或多个变换载荷)、一个 nonce 载荷和标识载荷。

杂凑载荷中消息摘要的计算方法如下：

HASH(1)= PRF(SKEYID_a,MsgID | Ni_b | SA [| IDi | IDr])

消息 2　响应方向发起方发送一个杂凑载荷、一个安全联盟载荷、一个 nonce 载荷和标识载荷。

杂凑载荷中消息摘要的计算方法如下：

HASH(2)= PRF(SKEYID_a,MsgID | Ni_b |SA | Nr_b [| IDi | IDr])

消息 3　发起方向响应方发送一个杂凑载荷，用于对前面的交换进行鉴别。

杂凑载荷中消息摘要的计算方法如下：

HASH(3)= PRF(SKEYID_a,0 | MsgID | Ni_b | Nr_b)

最后，会话密钥素材定义为：

KEYMAT = PRF(SKEYID_d, protocol | SPI | Ni_b | Nr_b)

其中，protocol 和 SPI 从协商得到的 ISAKMP 建议载荷中选取。

用于加密的会话密钥和用于完整性校验的会话密钥按照算法要求的长度从 KEYMAT 中依次选取。先选取用于加密的会话密钥，后选取用于完整性校验的会话密钥。

当 PRF 函数的输出长度小于 KEYMAT 需要的密钥素材长度时，需要利用反馈及连接方法加以扩展，直到满足对密钥长度的要求为止。即：

KEYMAT = K1 | K2 | K3 | ...

其中：

K1 = PRF(SKEYID_d, protocol | SPI | Ni_b | Nr_b)

K2 = PRF(SKEYID_d, K1 | protocol | SPI | Ni_b | Nr_b)

K3 = PRF(SKEYID_d, K2 | protocol | SPI | Ni_b | Nr_b)

...

单个 SA 协商产生两个安全联盟——一个入，一个出。每个 SA(一个由发起方选择，另一个由响应方选择)的不同的 SPI 保证了每个方向都有一个不同的 KEYMAT。由 SA 的目的地选择的 SPI，被用于衍生该 SA 的 KEYMAT。

5.1.2.3　ISAKMP 信息交换

如果 ISAKMP 安全联盟已经建立，则 ISAKMP 信息交换过程如下所示：

发起方	方向	响应方
HDR*，HASH(1)，N/D	—>	

其中 N/D 是一个 ISAKMP 通知载荷，或是一个 ISAKMP 删除载荷。HASH(1)的计算方法为：

HASH(1) = PRF(SKEYID_a, MsgID | N/D)

其中，MsgID 不能与同一个 ISAKMP SA 保护的其他第二阶段交换的 MsgID 相同。

这个消息的加密使用对称密码算法的 CBC 工作模式，其密钥使用 SKEYID_e，初始化向量 IV 是第一阶段的最后一组密文和 MsgID 进行 HASH 运算所得到的，即：

IV= HASH(第一阶段的最后一组密文 | MsgID)

消息的填充和第一阶段中的填充方式一样。

如果 ISAKMP 安全关联在信息交换时还没有建立,则消息以明文发送,即:

发起方	方向	响应方
HDR, N	--->	

5.1.3 NAT 穿越

IPSec 穿越 NAT 特性让 IPSec 数据流能够穿越网络中的 NAT 设备。NAT 穿越由 3 个部分组成:首先判断通信的双方是否支持 NAT 穿越,其次检测双方之间的路径上是否存在 NAT,最后决定如何使用 UDP 封装来处理 NAT 穿越。

实现 NAT 穿越的 NAT_D 载荷分别添加在第一阶段交换过程中消息 3 和消息 4 的载荷之后,这些载荷是独立的,不参与交换过程的所有密码运算。支持 NAT 穿越的第一阶段交换过程如下:

消息序列	发起方	方向	响应方
1	HDR,SA, VID	--->	
2		<---	HDR, SA, VID
3	HDR, XCHi, SIGi, NAT_D, NAT_D	--->	
4		<---	HDR, XCHr, SIGr,NAT_D, NAT_D
5	HDR * #,HASHi	--->	
6		<---	HDR * #,HASHr

注:#标志说明如果 NAT 存在,这些包将被发送到修改后的端口。

如果需要,NAT_OA 载荷分别添加在第二阶段交换过程中消息 1 和消息 2 的载荷之后,同第二阶段的消息载荷一起参与密码运算。

实现 NAT 穿越的处理过程和消息格式按 RFC3947 的规定执行。

5.1.4 密钥交换的载荷格式

5.1.4.1 消息头格式

密钥交换协议消息由一个定长的消息头和不定数量的载荷组成。消息头包含着协议用来保持状态并处理载荷所必须的信息。

ISAKMP 的头格式如图 1 所示。

图 1 ISAKMP 头格式

发起方 cookie:这个字段是一个唯一的 8 字节比特串,由发起方随机生成。

响应方 cookie:这个字段是一个唯一的 8 字节比特串,由响应方随机生成。

cookie 的生成方法应参照 RFC 2408 2.5.3 要求生成。

下一个载荷:这个字段为 1 个字节,说明消息中的第一个载荷的类型。载荷类型的定义如表 1

所示。

表 1　载荷类型的定义

下一个载荷	值
无（None）	0
安全联盟（Security association）	1
建议（Proposal）	2
变换（Transform）	3
密钥交换（Key exchange）	4
标识（Identification）	5
证书（Certificate）	6
证书请求（Certificate Request）	7
杂凑（HASH）	8
签名（Signature）	9
Nonce	10
通知（Norigication）	11
删除（Delete）	12
厂商（Vendor）	13
属性载荷	14
NAT_D	20
NAT_OA	21
对称密钥载荷（SK）	128
保留（Reserved）	15～19、22～127
私有使用（PrivateUse）	129～255

版本号：这个字段为 1 个字节，其中 0～3 位表示主版本号，4～7 位表示次版本号。本标准规定主版本号为 1，次版本号为 1。

交换类型：这个字段为 1 个字节，说明组成消息的交换的类型。交换类型的定义如表 2 所示。

表 2　交换类型的定义

交换类型	分配的值
无（None）	0
基本（Base）	1
身份保护（Identity protection）	2
仅鉴别（Authentication only）	3
信息（Informational）	5
将来使用（Future use）	6～31
DOI 具体使用	32～239
私有使用（Private use）	240～255

本标准规定密钥交换第一阶段使用的交换类型为身份保护类型即主模式，其值为 2。第二阶段交

换使用的快速模式所分配的值为32。

标志:这个字段的长度为1个字节,说明为密钥交换协议设置的具体选项。目前使用了这个域的前3个比特,其他比特在传输前被置为0。具体定义如下:

——加密比特:这是标志字段中的最低有效比特。当这个比特被置为1时,该消息头后面所有的载荷都采用ISAKMP SA中指定的密码算法加密。当这个比特被置为0时,载荷不加密。

——提交比特:这是标志字段的第2个比特,本标准中其值为0。

——仅鉴别比特:这是标志字段的第3个比特,本标准中其值为0。

消息ID:这个字段的长度为4字节,第一阶段中该字段为0,在第二阶段为发起方生成的随机数。它作为唯一的消息标志,用于在第二阶段的协商中标识协议状态。

长度:这个字段的长度为4字节,以字节为单位标明包含消息头和载荷在内的整个消息长度。

5.1.4.2 通用载荷头

每个载荷由通用载荷头开始。通用载荷头定义了载荷的边界,所以就可以联接不同的载荷。通用载荷头的定义如图2所示。

下一个载荷	保留	载荷长度

图2 通用载荷头格式

下一个载荷:这个字段的长度为1个字节,标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个,则该字段将被置为0。载荷类型由表1定义。

保留:这个字段的长度为1个字节,其值为0。

载荷长度:这个字段的长度为2个字节,以字节为单位标明包含通用载荷头在内的整个载荷长度。

5.1.4.3 安全联盟载荷

安全联盟载荷用于协商SA,并且指定协商所基于的解释域DOI。安全联盟的格式依赖于他使用的DOI,本载荷的类型值为1。安全联盟载荷的格式如图3所示。

下一个载荷	保留	载荷长度
解释域(DOI)		
情形		

图3 安全联盟载荷格式

下一个载荷:这个字段的长度为1个字节,标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个,则该字段将被置为0。载荷类型由表1定义。

保留:这个字段的长度为1个字节,其值为0。

载荷长度:这个字段的长度为2个字节,以字节为单位标明整个安全联盟载荷的长度,计算范围包括SA载荷、所有建议载荷和所有与被提议的安全联盟有关的变换载荷。

解释域(DOI):这个字段长度为4个字节,其值为无符号整数,它指定协商所基于的DOI,这个字段的值为1。

情形:这个字段长度为4个字节,表明协商发生时的情形,用来决定需要的安全服务的信息。定义如下:

——SIT_IDENTITY_ONLY:其值为1。表明SA将由一个相关的标识载荷中的源标识信息来标识。

——SIT_SECRECY:其值为2。表明SA正在一个需经标记的秘密的环境中协商。

——SIT_INTEGRITY:其值是4。表明SA正在一个须经标记的完整性环境中协商。

本标准默认采用SIT_IDENTITY_ONLY情形。

5.1.4.4 建议载荷

建议载荷用于密钥交换的发起方告知响应方它优先选择的安全协议以及希望协商中的SA采用的相关安全机制,本载荷的类型值为2。建议载荷的格式如图4所示。

下一个载荷	保留	载荷长度	
建议号	协议ID	SPI长度	变换数
变长的SPI			

图4 建议载荷格式

下一个载荷:这个字段的长度为1个字节,如果后面还有建议载荷,其值为2,否则应为0。

保留:这个字段的长度为1个字节,其值为0。

载荷长度:这个字段的长度为2个字节,以字节为单位标明整个建议载荷的长度。计算范围包括包括通用载荷头、建议载荷和所有与该建议有关的变换载荷,该长度仅用于标明本建议载荷的长度。

建议号:这个字段的长度为1个字节,标明本建议载荷的建议编号。多个建议的建议号相同标明这些建议是"逻辑与"的关系,不同标明这些建议是"逻辑或"的关系。单调递增的建议号表示对建议的优先选择顺序,建议号越小优先权越高。

协议ID:这个字段的长度为1个字节,标明协议标识符。协议标识符的定义如表3所示。

表3 协议标识符的定义

协议标识符	描　述	值
RESERVED	未分配	0
PROTO_ISAKMP	ISAKMP的协议标识符	1
PROTO_IPSec_AH	AH的协议标识符	2
PROTO_IPSec_ESP	ESP的协议标识符	3
PROTO_IPCOMP	IP压缩的协议标识符	4

SPI长度:这个字段的长度为1个字节,以字节为单位标明SPI的长度。在第一阶段该长度为0,在第二阶段该长度为4。

变换数:这个字段的长度为1个字节,标明建议的变换载荷个数。

变长的SPI:在第一阶段没有这个字段,在第二阶段这个字段的长度为4个字节,其内容是该建议的提出者产生的随机数。

5.1.4.5 变换载荷

变换载荷用于密钥交换的发起方告知响应方为一个指定的协议提供不同的安全机制,本载荷的类型值为3。变换载荷的格式如图5所示。

下一个载荷	保留	载荷长度
变换号	变换 ID	保留 2
SA 属性		

图 5　变换载荷格式

下一个载荷：这个字段的长度为 1 个字节，如果后面还有变换载荷，其值为 3，否则应为 0。

保留：这个字段的长度为 1 个字节，其值为 0。

载荷长度：这个字段的长度为 2 个字节，以字节为单位标明本变换载荷的长度。计算范围包括通用载荷头、变换载荷和所有的 SA 属性载荷。

变换号：这个字段的长度为 1 个字节，标明本变换载荷的变换编号。单调递增的变换号表示对变换的优先选择顺序，变换号越小优先权越高。

变换 ID：这个字段的长度为 1 个字节，标明建议协议的变换标识符。在第一阶段该字段的值为 1，在第二阶段根据不同的协议选用不同的变换 ID。AH 协议的变换 ID 的定义如表 4 所示，ESP 协议的变换 ID 的定义如表 5 所示。

表 4　AH 协议的变换 ID 的定义

变换 ID	描　　述	值
RESERVED	未使用	0～1
AH_SHA	使用 SHA-1 杂凑算法的 HMAC	3
AH_SM3	使用带 256 比特 SM3 密码杂凑算法的 HMAC	20

表 5　ESP 协议的变换 ID 的定义

变换 ID	描　　述	值
RESERVED	未使用	0
ESP_SM4	SM4 分组密码算法	127
ESP_SM1	SM1 分组密码算法	128

保留 2：这个字段的长度为 2 个字节，其值为 0。

SA 属性：该字段的长度是可变的，标明本变换的 SA 属性。该字段的具体定义见本标准 5.1.4.6。

5.1.4.6　SA 属性载荷

SA 属性载荷只能用于变换载荷之后，并且没有通用载荷头，用于表示 SA 属性的数据结构，本载荷的类型值为 14。SA 属性载荷的格式如图 6 所示。

	属性类型	属性值

	属性类型	属性长度
属性值		

图 6　SA 属性载荷格式

属性类型：这个字段的长度为 2 个字节，标明属性类型。该字段的最高有效比特（比特 0）如果为 0，

属性值是变长的，并且本载荷有 3 个字段，分别是属性类型、属性长度和属性值。如果属性类型最高有效比特为 1，属性值是定长的并且本载荷仅有 2 个字段，分别是属性类型和属性值。如果属性类型是变长的，并且属性值能在两个字节中表示，那么变长的属性可以用定长表示。

第一阶段密钥交换属性类型的定义如表 6 所示。

表 6　第一阶段密钥交换属性类型的定义

分　类	值	长　度
加密算法	1	定长
HASH 算法	2	定长
鉴别方式	3	定长
交换群描述	4	定长
交换群类型	5	定长
群素数/不可约多项式	6	变长
群产生器 1	7	变长
群产生器 2	8	变长
群曲线 A	9	变长
群曲线 B	10	变长
SA 生存期类型	11	定长
SA 生存期（SA Life Duration）	12	变长
伪随机函数(PRF)	13	定长
密钥长度	14	定长
字段大小	15	定长
群顺序	16	变长
块大小	17	定长
非对称算法类型	20	定长

第二阶段密钥交换属性类型的定义如表 7 所示。

表 7　第二阶段密钥交换属性类型的定义

分　类	值	长　度
SA 生存类型（SA Life Type）	1	定长
SA 生存期（SA Life Duration）	2	变长
组描述（Group Description）	3	定长
封装模式（Encapsulation Mode）	4	定长
鉴别算法（Authentication Algorithm）	5	定长
密钥长度（Key Length）	6	定长
密钥轮数（Key Rounds）	7	定长
压缩字典长度（Compress Dictionary Size）	8	定长
私有压缩算法（Compress Private Algorithm）	9	变长

属性值：这个字段如果是定长的，其长度为 2 个字节。如果是变长的，其长度由属性长度字段指定。
属性长度：当属性值是变长时，该字段标明属性值的长度。
第一阶段加密算法属性值的定义如表 8 所示。

表 8　第一阶段加密算法属性值的定义

可选择算法的名称	描述	值
ENC_ALG_SM1	SM1 分组密码算法	128
ENC_ALG_SM4	SM4 分组密码算法	129

第一阶段密码杂凑算法属性值的定义如表 9 所示。

表 9　第一阶段密码杂凑算法属性值的定义

名　称	描　述	值
HASH_ALG_SHA	SHA-1 密码杂凑算法	2
HASH_ALG_SM3	SM3 密码杂凑算法	20

第一阶段鉴别方式属性值的定义如表 10 所示。

表 10　第一阶段鉴别方式属性值的定义

名　称	描　述	值
AUTH_METHOD_DE	公钥数字信封鉴别方式	10

SA 生存期类型属性值的定义适用于第一阶段和第二阶段，如表 11 所示。

表 11　SA 生存期类型属性值的定义

名　称	描　述	值
SA_LD_TYPE_SEC	秒	1
SA_LD_TYPE_KB	千字节	2

第一阶段公钥算法类型属性值的定义如表 12 所示。

表 12　第一阶段公钥算法类型属性值的定义

名　称	描　述	值
ASYMMETRIC_RSA	RSA 公钥密码算法	1
ASYMMETRIC_SM2	SM2 椭圆曲线密码算法	2

第二阶段封装模式属性值的定义如表 13 所示。

表 13　第二阶段封装模式属性值的定义

名　称	描　述	值
RESERVED	使用	0
ENC_MODE_TUNNEL	隧道模式	1
ENC_MODE_TRNS	传输模式	2
ENC_MODE_UDPTUNNEL_RFC	NAT 穿越隧道模式	3
ENC_MODE_UDPTRNS_RFC	NAT 穿越传输模式	4

第二阶段鉴别算法属性值的定义如表 14 所示。

表 14　第二阶段鉴别算法属性值的定义

名　称	描　述	值
RESERVED	使用	0
HMAC_SHA	SHA-1 密码杂凑算法的 HMAC	2
HMAC_SM3	SM3 密码杂凑算法的 HMAC	20

5.1.4.7　标识载荷

标识载荷用于通信双方交换身份信息，该信息用于确认通信双方的身份，本载荷的类型值为 5。标识载荷的格式如图 7 所示。

图 7　标识载荷格式

下一个载荷：这个字段的长度为 1 个字节，标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个，则该字段将被置为 0。载荷类型由表 1 定义。

保留：这个字段的长度为 1 个字节，其值为 0。

载荷长度：这个字段的长度为 2 个字节，以字节为单位标明包含通用载荷头在内的整个载荷长度。

标识类型：这个字段的长度为 1 个字节，标明标识数据字段中的身份信息类型。标识类型的定义如表 15 所示。

表 15　标识类型的定义

ID 类型	描　述	值
RESERVED	未使用	0
ID_IPv4_ADDR	一个单独的 4 字节 IPv4 地址	1
ID_FQDN	完全合格的域名字符串	2
ID_USER_FQDN	完全合格的用户名字符串	3
ID_IPv4_ADDR_SUBNET	带有 4 字节子网掩码的 IPv4 地址	4

表 15（续）

ID类型	描　述	值
ID_IPv6_ADDR	一个单独的 16 字节 IPv6 地址	5
ID_IPv6_ADDR_SUBNET	一个带有 16 字节子网掩码的 IPv6 地址	6
ID_IPv4_ADDR_RANGE	一个 IPv4 的地址范围	7
ID_IPv6_ADDR_RANGE	一个 IPv6 的地址范围	8
ID_DER_ASN1_DN	一个 ASN.1X.500 的文本编码	9
ID_DER_ASN1_GN	一个 ASN.1X.500 的二进制编码	10
ID_KEY_ID	用于传递特定厂商信息的字节流	11

在第一阶段可以使用的标识类型为：

ID_IPv4_ADDR

ID_IPv6_ADDR

ID_DER_ASN1_DN

ID_DER_ASN1_GN

ID_FQDN

ID_USER_FQDN

ID_KEY_ID

在第二阶段可以使用的标识类型为：

ID_IPv4_ADDR

ID_IPv6_ADDR

ID_IPv4_ADDR_SUBNET

ID_IPv6_ADDR_SUBNET

ID_IPv4_ADDR_RANGE

ID_IPv6_ADDR_RANGE

协议 ID：这个字段的长度为 1 个字节，标明一个 IP 协议的上层协议号。值为 0 表明忽略这个字段，在第一阶段这个值应为 0。在第二阶段是用户配置的安全策略五元组的协议，值为 0 表明忽略这个字段。

端口：这个字段的长度为 2 个字节，标明一个上层协议的端口。值为 0 表明忽略这个字段，在第一阶段这个值应为 0。在第二阶段是用户配置的安全策略五元组的端口，值为 0 表明忽略这个字段。

标识数据：这个字段是变长的，标明与 ID 类型字段相对应的标识信息。

5.1.4.8　证书载荷

证书载荷用于通信双方交换证书以及证书相关信息，本载荷的类型值为 6。

证书载荷的格式如图 8 所示。

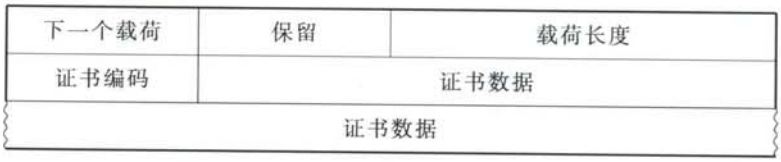

图 8　证书载荷格式

下一个载荷：这个字段的长度为 1 个字节，标识了本载荷后下一个载荷的类型。如果当前载荷是最