Protocolo IPSEC → (*ISAKMP*)

Por Alejandro Corletti (acorletti@hotmail.com)

- **Protocolos de seguridad. Asociaciones de seguridad.**
- **Administración de claves (IKE: Internet Key Exchange).**
- **(Algoritmos de autenticación y encriptado).**

Exposición: **Se realizará un muy breve repaso de IPSec para abordar el tema concreto de ISAKMP por medio de un ejemplo práctico.**

I. IPSec.

- Conjunto de RFC.
- Contempla su implementación tanto con la Versión 4 como con la 6 del protocolo IP.
- IPSec puede ser empleado para proteger uno o más caminos entre:

  - pares de host,
  - host y Gateway de seguridad
  - pares de Gateway de seguridad.

- El conjunto de servicios que IPSec puede proveer incluye:

  - Control de accesos.
  - Integridad no orientada a la conexión.
  - Autenticación de origen de datos.
  - Rechazo o reenvío de paquetes.
  - Confidencialidad.
  - Negociación de Compresión IP.

Los componentes fundamentales de esta arquitectura son:

- 1. Protocolos de seguridad: AH (Autentication Header) [RFC-2402] y ESP (Encapsulation Security Payload) [RFC-2406].
- 2. Asociaciones de seguridad (SA: Security Asociation).
- 3. IKE (Internet Key Exchange) [RFC-2409].
- 4. Algoritmos de autenticación y encriptado.

1.1. AH (Authentication Header) [RFC-2402]:

AH puede ser implementado solo, en combinación con ESP o anidado en el modo túnel de IPSec.

Los servicios de seguridad que ofrece pueden ser entre:

- Dos Host.
- Un Host y un Gateway de seguridad.
- Dos Gateway de seguridad.

En el caso de IPv4, el campo protocolo 51d → AH

1.2. ESP: Encapsulation Security Payload) [RFC-2406]:

ESP está diseñado para proveer servicios de seguridad a IPv4 e IPv6.
ESP provee confidencialidad, autenticación de origen de datos, integridad y servicio anti-réplica.
Estos servicios son seleccionados al establecerse la asociación de seguridad (SA) .

En el caso de IPv4, el campo protocolo 50d → ESP.

2. Asociaciones de seguridad (SA: Security Association).

Una SA es una clase de conexión que permite establecer los servicios de seguridad del tráfico.
En cada SA los servicios de seguridad pueden hacer uso de AH o ESP pero no de ambos.
Para utilizar los dos, se deberá establecer dos SA.
Una SA es unívocamente identificada por tres valores:

- SPI (Index Parameter Security).
- Dirección IP destino.
- Identificador de protocolo de seguridad (AH o ESP).

Se pueden definir dos tipos de SA:

2.1. Modo transporte: Se trata de una SA entre dos host.

2.2. Modo túnel: Se trata de una SA aplicada a un túnel IP.
En este modo existen dos encabezados IP, uno que es el *externo* que especifica los datos para llegar al destino del túnel y otro *interno* a este que detalla el destino final.

Un host debe soportar ambos modos, un Gateway de seguridad sólo debe soportar modo túnel.

3. Administración de claves (IKE: Internet Key Exchange) [RFC-2409].

IPSec impone el soporte para dos tipos de administración de claves:

a. Manual: Configuración personal.

b. Automático:

El protocolo por defecto que propone IPSec es IKE (Internet Key Exchange), sin embargo otros protocolos pueden ser seleccionados.

Cuando estos protocolos son empleados, la salida de los mismos pueden generar múltiples claves, las cuales sirven para:

- Algoritmos criptográficos que usan múltiples claves.
- Algoritmos de autenticación que usan múltiples claves.
- Combinaciones de ambos.

3.1. IKE:

La RFC-2409 describe un protocolo híbrido cuyo propósito es negociar y proveer material de claves autenticado para SA de una manera protegida.

IKE define tres elementos fundamentales:

- OAKLEY [RFC-2412]: Define una serie de "modos" de intercambio de claves detallando los servicios que provee cada uno.

- SKEME (Secure Key Exchange Mechanism for Internet): Describe una técnica de intercambio de claves muy versátil que provee anonimato, repudio y rápido refresco de claves.

- ISAKMP [RFC-2408] (Internet Security Association and Key Management Protocol): Provee un entorno para autenticación e intercambio de claves, pero no los define, sólo se limita a establecer las fases a seguir. Estas fases son dos.

IKE propone dos métodos básicos para establecer un intercambio de claves autenticado:

a. **Modo Principal** (Obligatorio): Sólo se emplea en la fase uno de ISAKMP. Es una instancia de ISAKMP para proteger el intercambio.

b. **Modo agresivo** (Optativo): Sólo se emplea en la fase uno de ISAKMP. Es también una instancia de ISAKMP, y funciona de la siguiente manera:

Existe también un modo rápido (Sólo se emplea en la fase dos de ISAKMP) para la refrescar las claves y SA, el cual no es un intercambio completo, pero es usado como parte de los procesos anteriores.

En modo principal o agresivo están permitidos cuatro métodos de autenticación:

- Firma digital.
- Dos métodos de clave pública.
- Secreto precompartido.

3.2. ISAKMP [RFC-2408] (Internet Security Association and Key Management Protocol):

Este protocolo define los pasos necesarios para establecer una SA (Security Association), el establecimiento y mantenimiento de todas las claves necesarias para la familia de protocolos TCP/IP en modo seguro.

Se desarrolla a continuación un ejemplo práctico tomado de la realidad en el establecimiento de una VPN por medio del software PGP, que implementa todos los estándares presentados por ISAKMP.

EJEMPLO:

a. Se presenta primero la captura de las 9 tramas obtenidas por medio del Software Protocol Inspector de FLUKE:

1 15:07:01.047 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 144 (PC-110 PC-105)

2 15:07:01.876 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 108 (PC-105 PC-110)

3 15:07:01.978 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 268 (PC-110 PC-105)

4 15:07:02.035 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 273 (PC-105 PC-110)

5 15:07:02.193 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 1260 (PC-110 PC-105)

6 15:07:02.332 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 1244 (PC-105 PC-110)

7 15:07:02.513 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 220 (PC-110 PC-105)

8 15:07:02.521 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 148 (PC-105 PC-110)

9 15:07:02.529 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 60 (PC-110 PC-105)

A continuación se detalla el encabezado de la primera de ellas:

```
          trace  Mon 04/23/01 15:49:36  A:\establecim VPN.TXT

1  15:07:01.047  UDP  Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 144 (PC-110 PC-105)

ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
      ETHERNET: Destination address : 0020185751DC
          ETHERNET: .......0 = Individual address
          ETHERNET: ......0. = Universally administered address
      ETHERNET: Source address : 0020185751D2
          ETHERNET: .......0 = No routing information present
          ETHERNET: ......0. = Universally administered address
      ETHERNET: Frame Length : 178 (0x00B2)
      ETHERNET: Ethernet Type : 0x0800 (IP:  DOD Internet Protocol)
      ETHERNET: Ethernet Data: Number of data bytes remaining = 164 (0x00A4)
  IP: ID = 0xCD01; Proto = UDP; Len: 164
      IP: Version = 4 (0x4)
      IP: Header Length = 20 (0x14)
      IP: Service Type = 0 (0x0)
          IP: Precedence = Routine
          IP: ...0.... = Normal Delay
          IP: ....0... = Normal Throughput
          IP: .....0.. = Normal Reliability
      IP: Total Length = 164 (0xA4)
      IP: Identification = 52481 (0xCD01)
```

```
      IP: Flags Summary = 0 (0x0)
          IP: .......0 = Last fragment in datagram
          IP: ......0. = May fragment datagram if necessary
      IP: Fragment Offset = 0 (0x0) bytes
      IP: Time to Live = 128 (0x80)
      IP: Protocol = UDP - User Datagram
      IP: CheckSum = 0xED1D
      IP: Source Address = 192.168.255.110
      IP: Destination Address = 192.168.255.105
      IP: Data: Number of data bytes remaining = 144 (0x0090)
UDP:  Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 144 (0x90)
      UDP: Source Port = 0x01F4          → (0x01F4  = 500 decimal)
      UDP: Destination Port = 0x01F4     → (0x01F4  = 500 decimal)
      UDP: Total length = 144 (0x90) bytes
      UDP: CheckSum = 0x4A52
      UDP: Data: Number of data bytes remaining = 136 (0x0088)

00000:   00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:   00 A4 CD 01 00 00 80 11 ED 1D C0 A8 FF 6E C0 A8   .............n..
00020:   FF 69 01 F4 01 F4 00 90 4A 52 2C 39 B7 D9 45 6C   .i......JR,9..El
00030:   8E 20 00 00 00 00 00 00 00 00 01 10 02 00 00 00   . ..............
00040:   00 00 00 00 00 88 0D 00 00 5C 00 00 00 01 00 00   .........\......
00050:   00 01 00 00 00 50 01 01 00 02 03 00 00 24 01 01   .....P.......$..
00060:   00 00 80 01 00 06 80 02 00 02 80 03 00 02 80 04   ................
00070:   00 05 80 0B 00 01 00 0C 00 04 00 01 51 80 00 00   ............Q...
00080:   00 24 02 01 00 00 80 01 00 05 80 02 00 02 80 03   .$..............
00090:   00 02 80 04 00 02 80 0B 00 01 00 0C 00 04 00 01   ................
000A0:   51 80 00 00 00 10 4F 70 65 6E 50 47 50 31 30 31   Q.....OpenPGP101
```

000B0: 37 31 **71**

El primer detalle a tener en cuenta es que se trata de 9 tramas, las cuales según la RFC-2409 se deberían a 6 de la *Fase 1* de ISAKMP operando en *modo principal* y 3 de la *Fase 2.*

- Fase 1: (modo principal) [RFC-2409, 5.]:
  Las dos primeras dos tramas ***negocian Políticas.***
  La tercera y cuarta Valores públicos de ***Diffie-Hellman (D-H) y "nonce"***.
  La quinta y sexta Autentican el intercambio ***Diffie-Hellman (D-H)***.

```
          Initiator                                  Responder
         ----------                                 -----------
HDR, SA                                (1) -->
                                       <-- (2)     HDR, SA
HDR,KE,[HASH(1)] <IDii_b>PubKey_r,
                   <Ni_b>PubKey_r      (3) -->
                                                  HDR, KE, <IDir_b>PubKey_i,
                                       <-- (4)           <Nr_b>PubKey_i
HDR*, HASH_I                           (5) -->
                                       <-- (6)     HDR*, HASH_R
```

- Fase 2: Tres tramas de intercambio de Hash.

El segundo detalle es que todas operan en modo no orientado a la conexión con el protocolo UDP y acceden a los puertos fuente y destino 01F4 hex = 500 dec, tal cual lo propone la RFC .

ACLARACION: Se permiten cuatro métodos de autenticación: Firma digital, Dos formas de clave pública (en este caso se aprecia D-H), Secreto compartido.

b. Para comenzar a analizar el contenido básico del encabezado de ISAKMP, se detalla a continuación únicamente los valores en hexadecimal de los mismos, resumiendo los datos que transportan:

```
1    15:07:01.047  ( PC-110  PC-105)
00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 A4 CD 01 00 00 80 11 ED 1D C0 A8 FF 6E C0 A8   .............n..
00020:  FF 69 01 F4 01 F4 00 90 4A 52 2C 39 B7 D9 45 6C   .i......JR,9..El
00030:  8E 20 00 00 00 00 00 00 00 00 01 10 02 00 00 00   . ..............
00040:  00 00 00 00 00 88 0D 00 00 5C 00 00 00 01 00 00   .........\......
00050:  00 01 00 00 00 50 01 01 00 02 03 00 00 24 01 01   .....P.......$..
00060:  00 00 80 01 00 06 80 02 00 02 80 03 00 02 80 04   ................
00070:  00 05 80 0B 00 01 00 0C 00 04 00 01 51 80 00 00   ............Q...
00080:  00 24 02 01 00 00 80 01 00 05 80 02 00 02 80 03   .$..............
00090:  00 02 80 04 00 02 80 0B 00 01 00 0C 00 04 00 01   ................
000A0:  51 80 00 00 00 10 4F 70 65 6E 50 47 50 31 30 31   Q.....OpenPGP101
000B0:  37 31                                             71

2   15:07:01.876  ( PC-105  PC-110 )
00000:  00 20 18 57 51 D2 00 20 18 57 51 DC 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 80 1D 01 00 00 80 11 9D 42 C0 A8 FF 69 C0 A8   .........B...i..
00020:  FF 6E 01 F4 01 F4 00 6C 67 62 2C 39 B7 D9 45 6C   .n.....lgb,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 01 10 02 00 00 00   . ..ia...g......
00040:  00 00 00 00 00 64 0D 00 00 38 00 00 00 01 00 00   .....d...8......
00050:  00 01 00 00 00 2C 01 01 00 01 00 00 00 24 01 01   .....,.......$..
```

```
00060:  00 00 80 01 00 06 80 02 00 02 80 03 00 02 80 04   ................
00070:  00 05 80 0B 00 01 00 0C 00 04 00 01 51 80 00 00   ............Q...
00080:  00 10 4F 70 65 6E 50 47 50 31 30 31 37 31         ..OpenPGP10171
3    15:07:01.978    ( PC-110   PC-105 )

00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:  01 20 CE 01 00 00 80 11 EB A1 C0 A8 FF 6E C0 A8   . ...........n..
00020:  FF 69 01 F4 01 F4 01 0C D6 C7 2C 39 B7 D9 45 6C   .i........,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 04 10 02 00 00 00   . ..ia...g......
00040:  00 00 00 00 01 04 0A 00 00 C4 4B FE 71 3C ......................

4    15:07:02.035   ( PC-105   PC-110 )
00000:  00 20 18 57 51 D2 00 20 18 57 51 DC 08 00 45 00   . .WQ.. .WQ...E.
00010:  01 25 1E 01 00 00 80 11 9B 9D C0 A8 FF 69 C0 A8   .%...........i..
00020:  FF 6E 01 F4 01 F4 01 11 C6 7A 2C 39 B7 D9 45 6C   .n.......z,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 04 10 02 00 00 00   . ..ia...g......
00040:  00 00 00 00 01 09 0A 00 00 C4 81 8F 8F ..........................

5   15:07:02.193   ( PC-110    PC-105 )
00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:  05 00 CF 01 00 00 80 11 E6 C1 C0 A8 FF 6E C0 A8   .............n..
00020:  FF 69 01 F4 01 F4 04 EC 6F 1C 2C 39 B7 D9 45 6C   .i......o.,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 05 10 02 01 00 00   . ..ia...g......
00040:  00 00 00 00 04 E4 A5 7E 00 AA.....................................

6    15:07:02.332    ( PC-105    PC-110 )
00000:  00 20 18 57 51 D2 00 20 18 57 51 DC 08 00 45 00   . .WQ.. .WQ...E.
00010:  04 F0 1F 01 00 00 80 11 96 D2 C0 A8 FF 69 C0 A8   .............i..
```

```
00020:  FF 6E 01 F4 01 F4 04 DC F2 FA 2C 39 B7 D9 45 6C   .n........,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 05 10 02 01 00 00   . ..ia...g......
00040:  00 00 00 00 04 D4 CB 69 AF AA 0A                  .......i.....
```

7 15:07:02.513 (PC-110 PC-105)

```
00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 F0 D0 01 00 00 80 11 E9 D1 C0 A8 FF 6E C0 A8   .............n..
00020:  FF 69 01 F4 01 F4 00 DC CD 38 2C 39 B7 D9 45 6C   .i.......8,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 08 10 20 01 5C F8   . ..ia...g.. .\.
00040:  CD CC 00 00 00 D4 E8 7F BC                        .........
```

8 15:07:02.521 (PC-105 PC-110)

```
00000:  00 20 18 57 51 D2 00 20 18 57 51 DC 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 A8 20 01 00 00 80 11 9A 1A C0 A8 FF 69 C0 A8   .. ..........i..
00020:  FF 6E 01 F4 01 F4 00 94 89 FE 2C 39 B7 D9 45 6C   .n........,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 08 10 20 01 5C F8   . ..ia...g.. .\.
00040:  CD CC 00 00 00 8C B1 F9 48 4E 88                  ........HN.
```

9 15:07:02.529 (PC-11 PC-105)

```
00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 50 D1 01 00 00 80 11 E9 71 C0 A8 FF 6E C0 A8   .P.......q...n..
00020:  FF 69 01 F4 01 F4 00 3C E8 C3 2C 39 B7 D9 45 6C   .i.....<..,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 08 10 20 01 5C F8   . ..ia...g.. .\.
00040:  CD CC 00 00 00 34 54 C0 FD 08 00 8F BD AF A0 53   .....4T........S
00050:  8B 7E A3 41 2F E7 C9 B3 43 65 6C 2F 45 2C         .~.A/...Cel/E,
```

```
00020:  FF 69 01 F4 01 F4 00 3C E8 C3 2C 39 B7 D9 45 6C    .i.....<..,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 08 10 20 01 5C F8    . ..ia...g.. .\.
00040:  CD CC 00 00 00 34 54 C0 FD 08 00 8F BD AF A0 53    .....4T........S
```

- Cookie de inicio: 2C 39 B7 D9 45 6C 8E 20. función Hash sobre un valor generado desde las direcciones IP fuente y destino, los puertos fuente y destino, un valor aleatorio y la fecha y hora.
- Cookie de respuesta: En la primer trama es cero y luego E9 BF 69 61 84 F5 E2 67 08.
- Next Payload: Indica que tipo de mensaje sigue a este encabezado básico.
  Se pueden apreciar los siguientes valores:
  01: Security Association (SA) Fase 1 Negocian políticas.
  04: Key Exchange (KE) Fase 1 Intercambian D-H y "nonce".
  05: Identification (ID) Fase 1 Autentican intercambio D-H.
  08: Hash (HASH) Fase 2 Hash (3 tramas).
- Mayor Versión (4 bit): Mayor versión de ISAKMP en uso. La actual versión [RFC-2408], indica 1.
- Menor versión (4 bit): Menor versión de ISAKMP en uso. La actual versión [RFC-2408], indica 0.
- **Tipo de Intercambio:** Indica qué tipo de intercambio se está realizando, regula el orden ISAKMP. Los valores son: **02**: Protección de identidad (6 tramas) Fase 1.
  20 hex = 32 dec: Uso específico de DOI (Domain of Interpretation), (3 tramas) Fase 2.
- **Flags**: Indica opciones específicas de Criptografía. Autenticación o sincronismo, en este caso se emplearon: **00**: Texto simple (4 tramas).
  01: Criptografía (5 tramas).
- **Identidad del Mensaje:** Es un valor aleatorio empleado para la negociación durante la Fase 2. Se empleó aquí: **00 00 00 00:** Durante la Fase 1 este valor deberá ser 0 (6 tramas).
  5C F8 CD CC: Fase 2, identificador aleatorio.
- Longitud (4 Byte): Longitud de encabezado y datos:

CONCLUSIONES PARCIALES:

1) encabezado común en las 9 tramas, ***longitud fija de 28 Bytes***.

2) 6 tramas de fase 1 y 3 de fase 2.

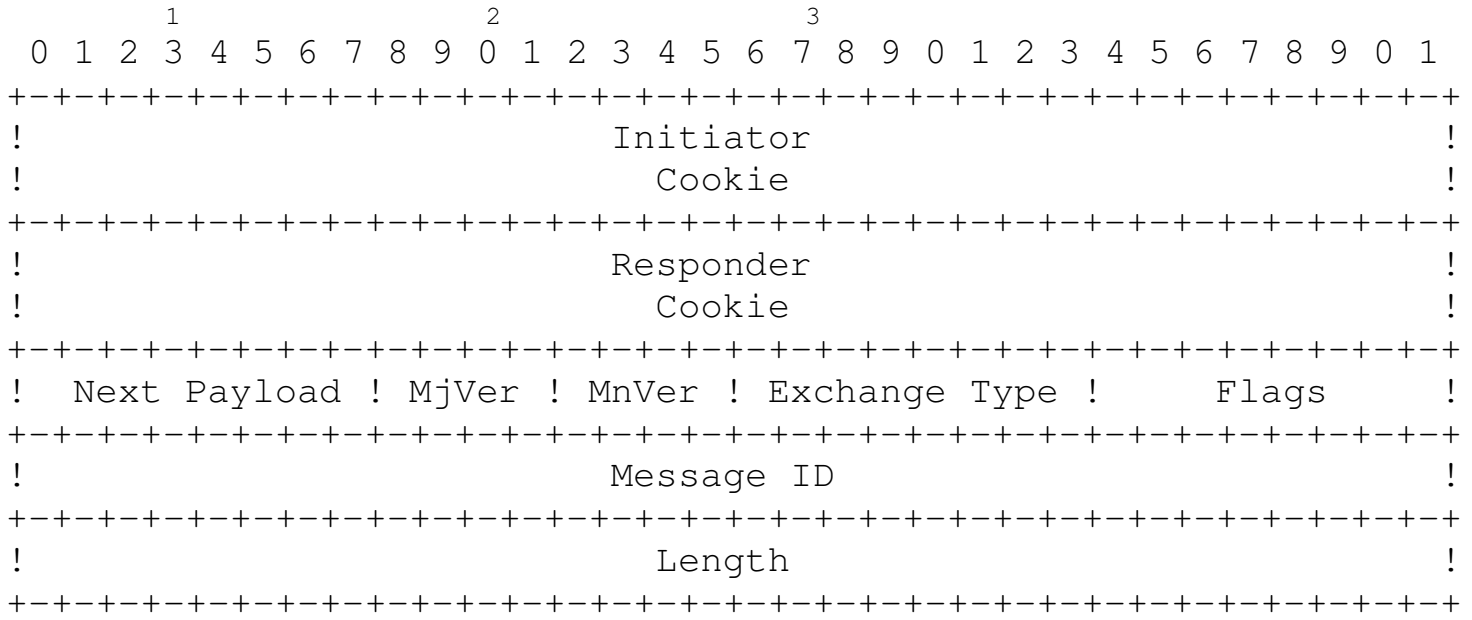
3) 2 tramas (SA), 2 tramas (KE), 2 tramas (ID) y 3 tramas (HASH).

4) 4 tramas en ***texto plano*** y 5 con ***criptografía***.

5) Las 3 tramas criptografiadas (últimas 3) tienen un ***identificador aleatorio***, las 6 anteriores *no*.

6) Las cookies de inicio y respuesta se mantienen en todas las tramas.

El encabezado básico de ISAKMP es el siguiente:



c. A continuación se analizan los encabezados de extensión:

```
1    15:07:01.047   ( PC-110   PC-105)
 00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00    . .WQ.. .WQ...E.
00010:  00 A4 CD 01 00 00 80 11 ED 1D C0 A8 FF 6E C0 A8    .............n..
00020:  FF 69 01 F4 01 F4 00 90 4A 52 2C 39 B7 D9 45 6C    .i......JR,9..El
00030:  8E 20 00 00 00 00 00 00 00 00 01 10 02 00 00 00    . ..............
00040:  00 00 00 00 00 88 0D 00 00 5C 00 00 00 01 00 00    .........\......
00050:  00 01 00 00 00 50 01 01 00 02 03 00 00 24 01 01    .....P.......$..
00060:  00 00 80 01 00 06 80 02 00 02 80 03 00 02 80 04    ................
00070:  00 05 80 0B 00 01 00 0C 00 04 00 01 51 80 00 00    ............Q...
00080:  00 24 02 01 00 00 80 01 00 05 80 02 00 02 80 03    .$..............
00090:  00 02 80 04 00 02 80 0B 00 01 00 0C 00 04 00 01    ................
000A0:  51 80 00 00 00 10 4F 70 65 6E 50 47 50 31 30 31    Q.....OpenPGP101
000B0:  37 31                                              71

2   15:07:01.876   ( PC-105   PC-110 )
00000:  00 20 18 57 51 D2 00 20 18 57 51 DC 08 00 45 00    . .WQ.. .WQ...E.
00010:  00 80 1D 01 00 00 80 11 9D 42 C0 A8 FF 69 C0 A8    .........B...i..
00020:  FF 6E 01 F4 01 F4 00 6C 67 62 2C 39 B7 D9 45 6C    .n.....lgb,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 01 10 02 00 00 00    . ..ia...g......
00040:  00 00 00 00 00 64 0D 00 00 38 00 00 00 01 00 00    .....d...8......
00050:  00 01 00 00 00 2C 01 01 00 01 00 00 00 24 01 01    .....,.......$..
00060:  00 00 80 01 00 06 80 02 00 02 80 03 00 02 80 04    ................
00070:  00 05 80 0B 00 01 00 0C 00 04 00 01 51 80 00 00    ............Q...
00080:  00 10 4F 70 65 6E 50 47 50 31 30 31 37 31          ..OpenPGP10171
```

- Encabezado básico ISAKMP (tratado en el punto anterior).

```
00040:  00 00 00 00 00 64 0D 00 00 38 00 00 00 01 00 00    .....d...8......
00050:  00 01 00 00 00 2C 01 01 00 01 00 00 00 24 01 01    .....,.......$..
```

1) **Security Association Payload:** Se emplea para negociar atributos, indicar DOI (Domain of Interpretation) y situaciones de la negociación. En este caso los valores son:

```
Trama 1:  0D 00 00 5C 00 00 00 01 00 00 00 01
Trama 2:  0D 00 00 38 00 00 00 01 00 00 00 01
```

- **Generic Payload Header** (4 Byte) :

  Next Payload (0D): Vendor ID, no se tiene en cuanta en esta fase ni el encabezado de Proposal Payload (Lila) ni el encabezado de Transform Payload (gris), pues son obligatorios. Por esto se define como próximo encabezado 0D que en este caso es OpenPGP10171

  Reservado (00): Deb ser 0.

  Length Payload (00 5C o 00 38): Longitud total de encabezados, incluyendo encabezado de Proposal Payload (Lila) y el encabezado de Transform Payload (gris). 00 5C hex = 92 dec, 00 38 hex = 56 dec, corresponden a la suma de los campos: verde, lila y gris.

- **DOI** (4 Byte) (00 00 00 01): El valor 1 corresponde a IPSec DOI.

- **Situation** (4 Byte) (00 00 00 01): Este campo está definido en la RFC-2407, en el punto 4.2 y en este caso significa SIT_IDENTITY_ONLY, con lo cual se especifica que la SA será identificada por la información de la fuente presente en el campo Identification Payload, es decir en las tramas 5 y 6.

```
00050:  00 01 00 00 00 2C 01 01 00 01 00 00 00 24 01 01   .....,.......$..
```

2) **Proposal Payload:** Información empleada durante la SA para asegurar el canal de comunicaciones.

Trama 1: 00 00 00 50 01 01 00 02
Trama 2: 00 00 00 2C 01 01 00 01

- **Next Payload** (00) : Último Proposal Payload.
- **Reservado** (00): Debe ser 0.
- **Payload Length** (00 50 o 00 2C): Longitud de encabezado más Payload , es decir todo lo lila, celeste y gris.
- **Cantidad de Proposal** (01): Contador monótono creciente
- **Identidad de protocolo** (01): Identifica PROTO_ISAKMP, es la protección de mensajes requerida durante la fase 1. Otros valores posibles son: 02 = PROTO_ IPSEC_AH,

  03 = PROTO_IPSEC_ESP y 04 = PROTO_IPCOMP.
- **Tamaño de SPI** (00): Este campo define el tamaño de un campo opcional que debería ir a continuación del campo siguiente (cantidad de transformadas) llamado SPI: Specifies Protocol Identifier, que en este caso por ser 00 indica que el campo SPI no existirá.
- **Cantidad de transformadas** (02 o 01): Indica cuántos encabezados de transformación le seguirán. Como se puede apreciar en la trama uno seguirán dos (el gris y el celeste) y en la trama 2, sólo uno.
- **SPI** (Variable): nulo pues Tamaño de SPI = 0.

3) **Transform Payload:** Contiene la información usada durante la negociación de la SA. Especifica que transformaciones (algoritmos) se emplearán para asegurar el canal de comunicaciones. Los campos son los siguientes:

```
Trama 1: 03 00 00 24 01 01 00 00 80 01 00 06 80 02 00 02 80 03 00 02
         80 04 00 05 80 0B 00 01 00 0C 00 04 00 01 51 80

         00 00 00 24 02 01 00 00 80 01 00 05 80 02 00 02 80 03 00 02
         80 04 00 02 80 0B 00 01 00 0C 00 04 00 01 51 80
```

- **Next Payload**: Sólo puede contener los valores 00 (Última) o 03 (existen más transform Payload).
- **Reservado**: Debe ser 00, 00.
- **Payload Length**: 0024, 0024.
- **Cantidad de transformaciones**: 01, 02.
- **ID de transformación:** 01, 01 identifica KEY_IKE.
- **Reservado 2**: 0000, 0000.
- **Atributos**: Son mínimo cuatro octetos:

- El primer bit: atributo básico o variable, al estar en 0 es variable y los atributos son TIPO/LONGITUD/VALOR, y al estar en 1 será básico, 80 y los atributos son TIPO/VALOR.
- Continúan dentro de estos dos octetos TIPO de atributo [Apéndice A RFC-2409 IKE].
- Si es básico (80), continúa VALOR que son dos octetos que indican la transformación [Apéndice A RFC-2409 IKE].
- Si es variable (00) se determina su LONGITUD y luego irá el campo VALOR. Idem básico.

80 01 00 06: básico, 01 = Encriptation, 00 06 = CAST-CBC.
80 02 00 02: básico, 02 = Hash Algorithm, 00 02 = SHA [FIPS-180-1].
80 03 00 02: básico, 03 = Authentication, 00 02 = DSS Signature.
80 04 00 05: básico, 04 = Group Description, 00 05 = Res IANA.
80 0B 00 01: básico, 0B = Lyfe Type, 00 01 = segundos.
00 0C 00 04 00 01 52 80: variable, 0C = Life Duration, 00 04 = Longitud 4 octetos,
00 01 52 80 = 15.280 segundos = 24 horas.

80 01 00 05: básico, 01 = Encriptation, 00 05 = 3DES-CBC.
80 04 00 02: básico, 04 = Groupe Description, 00 02 = 1024-bit MODP (modular exponentiation) group.

```
Trama 2: 00 00 00 24 01 01 00 00 80 01 00 06 80 02 00 02 80 03 00
         02 80 04 00 05 80 0B 00 01 00 0C 00 04 00 01 51 80
```

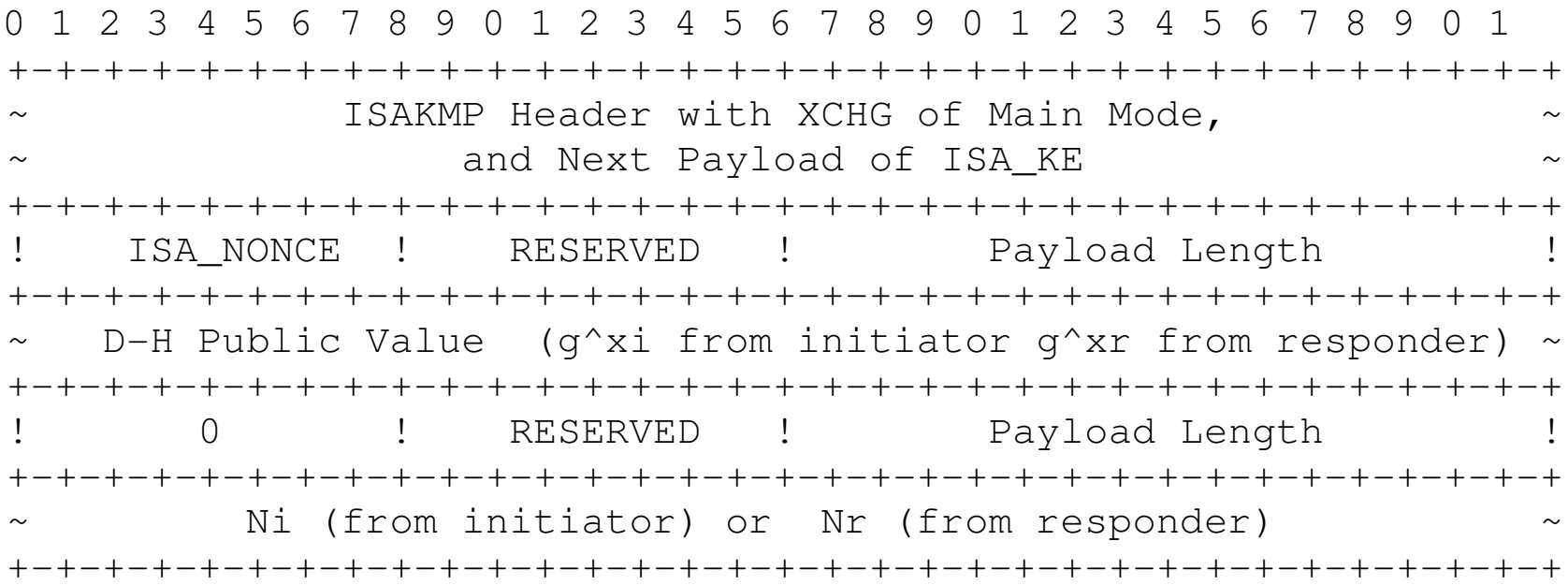
La PC-110 le propone dos transformaciones de encriptado **CAST y 3DES** y dos grupos **Res IANA y MODP**.
La PC-105 le afirma que empleará la primer transformada (**CAST**) y grupo **Reservado por IANA**.
El resto de los parámetros son para la SA a través de **firma digital** y **SHA**, duración será de 24 horas.

4) Vendedor:

```
00 00 00 10 4F 70 65 6E 50 47 50 31 30 31 37 31          ..OpenPGP10171
```

- **00**: variable.
- **00**: Vendedor.
- **0010** hex = 16 dec: Longitud.
- **4F 70 65 6E 50 47 50 31 30 31 37 31**: OpenPGP10171.

Las tramas 3 y 4 (KE) intercambiarán los valores de claves públicas de ambas entidades y dos valores aleatorios denominados “nonce”.

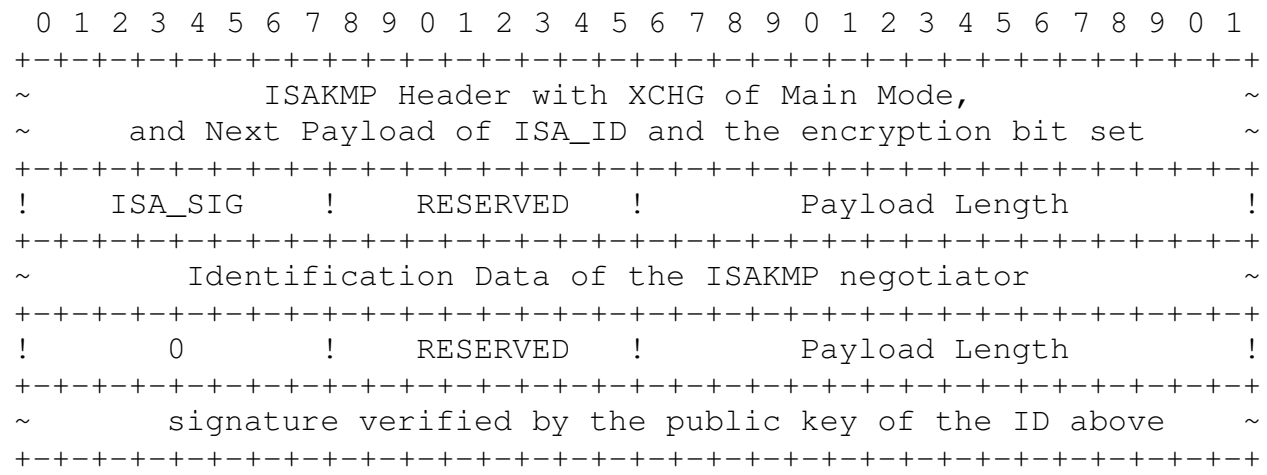


```
Trama 3  15:07:01.978 ( PC-110  PC-105 )
........Ethernet, IP, UDP, .....Encabezado báscio ISAKMP
........02 00 00 00  01 04 0A 00 00 C4 4B FE ..........    ..........K.q<..
00050:  .........CLAVE PÚBLICA PC-110 ..................    ..\).%(-#......
00100:  ...................84 61 51 F6 00 00 00 24 38 25    vo$..'.aQ....$8%
00110:  5C C3 B5 B3 9D 4C 4F 28 DC EF 07 2A C7 3C 6D 1F    \....LO(...*.<m.
00120:  CF BC 08 E0 7A E8 87 80 8A E4 5D DC E3 6C          ....z.....]..l

Trama 4   15:07:02. ( PC-105  PC-110 )
........Ethernet, IP, UDP, .....Encabezado báscio ISAKMP
........00 00 00 00 01 09 0A 00 00 C4 81 8F ............     ..............Ey
00050:  .........CLAVE PÚBLICA PC-105 ..................    ..\).%(-#......
00100:  ...................69 23 6C E2 07 00 00 24 B1 2A    ......i#l....$.*
00110:  9E BF 45 A9 5F 9E A1 9D A6 1B 8B 39 FA 3A D7 F4    ..E._......9.:..
00120:  74 7D DD 52 DC B4 CD FB DF 09 04 5A 0F DF 00 00    t}.R.......Z....
00130:  00 05 02                                           ...
```

- 0A: Identifica "nonce".
- 00: Reservado.
- 00 C4 hex = 196 dec: Longitud de Payload (incluye toda la clave pública más el primer encabezado verde).
- **Clave pública**: longitud 192 octetos = 1536 bit.
- 00 o 07: Grupo generador.
- 00: reservado.
- 00 24 hex = 36 dec: Longitud de payload.
- Nonce: número aleatorio.

Las tramas 5 y 6 (ID) firmarán digitalmente para dejar establecida la autenticación.
Al validar estas firmas, los secretos compartidos SKEYID_e y SKEYID_a son marcados como autenticados.
Estas dos tramas ya comienzan a encriptar sus datos pues ya poseen y verifican las claves públicas.
El encabezado de estas tramas es el siguiente:



En el caso de las tramas enviadas es:

```
Trama 5     15:07:02.193    ( PC-110   PC-105 )
........Ethernet, IP, UDP, ....Encabezado báscio ISAKMP
con el bit Flag =1 de encriptado...67 05 10 02 01 00 00 ...ia...g.....
00040:  00 00 00 00 04 E4 A5 7E..... Datos encriptados.................
```

```
Trama 6     15:07:02.332    ( PC-105   PC-110 )
........Ethernet, IP, UDP, ....Encabezado báscio ISAKMP
con el bit Flag =1 de encriptado...67 05 10 02 01 00 00   ...ia...g.....
00040:  00 00 00 00 04 D4 CB 67..... Datos encriptados.................
```

RESUMEN:

- **2 tramas (SA) *Negocian políticas*, fase 1.**
- **2 tramas (KE) *Intercambian claves públicas y "nonce"*, fase 1.**
- **2 tramas (ID) *Autentican el Intercambio D-H*, fase 1.**
- **3 tramas (HASH), fase 2.**
- **Exchange Type: 6 tramas (02) *Identity Protection*.**
  3 tramas (32) *Domain Of Interpretation*.
- **Flags: 4 tramas (00) *sin encriptar*.**
  5 tramas (01) *encriptado*.
- **Message ID: 6 tramas (0) fase 1**
  3 tramas (5C F8 CD CC) fase 2.

Las tramas 7, 8 y 9 son las que realizan el Hash y presentan encabezados similares a las dos anteriores, pues ya se encuentran encriptados todos los datos. Por esta causa no son detalladas a continuación.