Grupo de Trabajo en Red
Request for Comments: 2408
Categoría: Pila de estándares

D. Maughan
National Security Agency
M. Schertler
Securify, Inc.
M. Schneider
National Security Agency
J. Turner
RABA Technologies, Inc.

Noviembre 1998

Traducción al castellano: Agosto 2005
Hugo Adrian Francisconi <adrianfrancisconi@yahoo.com.ar>

Protocolo de Gestión de Claves y Asociaciones de Seguridad en Internet (ISAKMP)

Estado de este documento

Este documento especifica un protocolo de Internet en vías de estandarización para la comunidad de Internet y solicita debate y sugerencias para mejorarlo. Por favor, remítase a la edición actual de "Estándares de Protocolos Oficiales de Internet" (STD 1) para conocer el estado de estandarización y status de este protocolo. La distribución de este memorándum es ilimitada.

Aviso de Copyright

Resumen

Este documento describe un protocolo que utiliza conceptos de seguridad necesarios para el establecimiento de Asociaciones de Seguridad (SA) y claves criptográficas en un entorno de Internet. Un protocolo que negocia, establece, modifica y cancela SAs y sus atributos es requerido para la Internet en desarrollo, donde existirán numerosos mecanismos de seguridad y varias opciones para cada mecanismo. El protocolo de seguridad de manejo de claves debe ser robusto para manejar la generación de claves públicas para la comunidad de Internet y los requerimientos de claves privadas para esas redes privadas con ese requerimiento. El Protocolo para el manejo de claves y Asociaciones de Seguridad (ISAKMP) define los procedimientos para autentificar comunicaciones entre usuarios, la

creación y administración de Asociaciones de Seguridad, las técnicas de generación de claves y atenuación de amenazas (como por ejemplo, denegación de servicio y ataques de reenvío). Todo esto es necesario para entablar y mantener comunicaciones seguras (A través de los servicios de seguridad IP o cualquier otro protocolo de seguridad) en un entorno de Internet.

Lista de contenido

Lista de Imágenes

1 Introducción

Este documento describe el Protocolo de Gestión de Claves y Asociaciones de Seguridad en Internet (ISAKMP). ISAKMP combina los conceptos de seguridad de autentificación, administración de claves, y de asociaciones de seguridad para establecer la seguridad requerida por el gobierno, comercio, y comunicaciones privadas en Internet.

El Protocolo de Gestión de Claves y Asociaciones de Seguridad en Internet (ISAKMP) define los procedimientos y los formatos de los paquetes para establecer, negociar, modificar y eliminar las

Asociaciones de Seguridad (SA). Las SAs contienen toda la información requerida para la ejecución de varios servicios de seguridad de red, tales como los servicios de la capa IP (tales como la cabecera de autentificación y la cabecera de carga de seguridad encapsulada), trasporte o servicios de la capa aplicación o autoprotección del tráfico de negociación. ISAKMP define las cargas para el intercambio de generación de claves y autentificación de datos. Estos formatos proporcionan un marco consistente para la transferencia de claves y autentificación de datos que es independiente de la técnica de generación de claves algoritmo de encriptación, y mecanismo de autentificación.

ISAKMP es diferente al protocolo de intercambio de claves para separar claramente los detalles de la administración de SA (y administración de claves) de los detalles de intercambio de claves. Puede haber diferentes protocolos de intercambio de claves, cada uno con propiedades de seguridad diferente. Sin embargo, un marco común es requerido para acordar el formato de los atributos de la SA, y para la negociación, modificación, y cancelación de SAs. ISAKMP proporciona este marco común.

La separación de la funcionalidad en tres partes agrega complejidad al análisis de seguridad a una implementación de ISAKMP completa. No obstante, la separación es importante para la interoperatibilidad entre sistemas con requerimientos de seguridad diferentes, y debería también simplificar el análisis de una futura evolución de un servidor ISAKMP.

ISAKMP está diseñado para soportar la negociación de SAs de los protocolos de seguridad de todas las capas de la pila de protocolos de red (IPsec, TLS, TLSP, OSPF, etc.). Centralizando la administración de SAs, ISAKMP reduce el costo de la funcionalidad duplicada dentro de cada protocolo de seguridad. ISAKMP también puede reducir el tiempo de inicio de conexión, negociando un conjunto de servicios al mismo tiempo.

El resto de la sección 1 establece la motivación para la negociación de seguridad y detalla los componentes principales de ISAKMP, es decir SA y administración, autentificación, criptografía de clave pública y otros temas relacionados. La Sección 2 presenta la terminología y los conceptos relacionados con ISAKMP. La Sección 3 describe los diferentes formatos de carga ISAKMP. La Sección 4 describe como están compuestas las cargas ISAKMP y los tipos de intercambios para establecer SAs y realizar intercambios de claves en un modo autentificado. La modificación, cancelación, y notificación de error de una SA, son también analizados en esa sección. La Sección 5 describe el procesamiento de cada carga dentro del contexto de los intercambios de ISAKMP, incluyendo el manejo de errores y temas

relacionados. Los apéndices proporcionan los valores de los atributos, necesarios para ISAKMP y los requisitos para definir un nuevo Dominio de Interpretación (DOI) dentro de ISAKMP.

1.1 Requisitos Terminológicos

Las palabras DEBE, NO DEBE, REQUERIDO, PODER, NO PODER, DEBERÍA, NO DEBERÍA, RECOMENDADO, PUEDE y OPCIONAL, cuando aparezcan en este documento, deben interpretarse como se describen en [RFC-2119].

1.2 La Necesidad de Negociación

ISAKMP extiende la aseveración de [DOW92] en que la autentificación y los intercambios de claves deben ser combinados para mejorar la seguridad incluida en los intercambios de SA. Los servicios de seguridad requeridos para las comunicaciones dependen de la configuración de las redes individuales y del ambiente. Las organizaciones que forman Redes Privadas Virtuales (VPN), también conocidas como Intranet, necesitarán un conjunto de funciones de seguridad para las comunicaciones dentro de las VPN y posiblemente muchas funciones de seguridad diferentes para comunicaciones fuera de las VPN, para soportar geográficamente componentes organizativos separados, clientes, proveedores, subcontratistas (con sus propias VPNs), gobiernos, y otros. Los departamentos dentro de las grandes organizaciones requerirán un número de SA para separar y proteger los datos (por ejemplo, datos personales, datos de la compañía, etc.) en redes internas y en otras SAs para comunicarse dentro del mismo departamento. Usuarios móviles que quieren "llamar a casa" representan otro conjunto de requerimientos de seguridad. Estos requerimientos deben ser condicionados con un ancho de banda. Entidades más pequeñas pueden resolver sus requisitos de seguridad estableciendo "redes de confianza". Los intercambios de ISAKMP proporcionan a estas comunidades de red la capacidad de presentar usuarios con funciones de seguridad que el usuario soporta en un modo acordado, autentificado y protegido sobre un conjunto de atributos de seguridad en común, es decir una, SA ínter operable.

1.3 Qué Puede ser Negociado

Las Asociaciones de Seguridad deben soportar diversos algoritmos de encriptación, mecanismos de autentificación y algoritmos para el establecimiento de claves, para otros protocolos de seguridad, como así también para IPsec. Las Asociaciones de seguridad también deben soportar certificados orientados a host para los protocolos de capas inferiores y certificados orientados a usuarios para protocolos de capas superiores. Algoritmos y mecanismos independientes se requieren en aplicaciones tales como, e-mail, conexión remota, transferencia de

archivos, como así también sesiones orientadas a protocolos, protocolos de ruteo, y protocolos de capas de enlace. ISAKMP proporciona una SA común y protocolos de establecimiento de claves para esta gran variedad de protocolos de seguridad, aplicaciones, requerimientos de seguridad y ambientes de redes.

ISAKMP no está sujeto a ningún algoritmo criptográfico especifico, técnica de generación de claves o mecanismos de seguridad. Esta flexibilidad es beneficiosa por numerosas razones. Primero porque soporta ambientes de comunicaciones dinámicos descriptos anteriormente. Segundo independencia de los mecanismos de seguridad específicos y suministra a los algoritmos un mejor camino migratorio progresivo para mecanismos y algoritmos. Cuando mejores mecanismos de seguridad son desarrollados o nuevos ataques a algoritmos de encriptación actuales, mecanismos de autentificación o intercambios de generación de claves son descubiertos ISAKMP permitirá la actualización de algoritmos y mecanismos sin tener que desarrollar un nuevo KMP o mejorar el actual.

ISAKMP tiene requisitos básicos para su autentificación y componentes de intercambio de claves. Estos requerimientos protegen contra la denegación de servicio, el reenvío/reflexión, ataques en la trayectoria (man-in-the-middle), y ataques contra secuestro de la conexión. Esto es importante porque estos son los tipos de ataques que están dirigidos hacia los protocolos. El completo soporte de Asociaciones de Seguridad (SA), el cual proporciona mecanismos y algoritmos independientes, y protección de los protocolos contra amenazas son las fortalezas de ISAKMP.

1.4 Asociaciones de Seguridad y Administración

Una SA es una relación entre dos o más entidades que describe como las entidades utilizan los servicios de seguridad para comunicarse en forma segura. Esta relación esta representada por un conjunto de información que puede ser considerada como un contrato entre las entidades. La información debe ser acordada y compartida por todas las entidades. Algunas veces solo la información es referida como una SA pero esto es una ejemplificación física de la relación existente. La existencia de esta relación, representada por la información, es lo que proporciona la información de seguridad necesaria para que ínter-operen de forma segura. Todas las entidades se deben adherir a la SA para que sean posibles las comunicaciones seguras. Cuando atributos de SA se accesan, las entidades usan un puntero o un identificador que hace referencia a un SPI. [SEC-ARCH] proporciona detalles referentes a las definiciones de SA y SPI.

1.4.1 Asociaciones de Seguridad y Registraciones

Los atributos requeridos y recomendados para una SA IPsec (AH, ESP) están definidos en [SEC-ARCH]. Los atributos específicos para una SA IPsec incluyen, pero no están limitados a, mecanismos de autentificación, algoritmos criptográficos, modos de algoritmos, longitud de las claves, y el Vector de Inicialización (IV). Otros protocolos que proporcionen algoritmos y mecanismos independientes de seguridad DEBEN definir sus requerimientos para los atributos de las SAs. La separación de una definición específica de SA ISAKMP es importante para asegurar que ISAKMP pueda establecer SAs para todos los posibles protocolos de seguridad y aplicaciones.

NOTA: Vea [IPDOI] para un debate de los atributos de las SA que deberían ser considerados para las definiciones de un protocolo de seguridad o aplicaciones.

Para facilitar la rápida identificación de atributos específicos (por ejemplo, un algoritmo de encriptación específico) entre varias entidades se DEBEN designar identificadores de atributos y estos identificadores deben ser registrados por una autoridad central. La Autoridad de Asignación de Números en Internet (IANA) proporciona esta función para Internet.

1.4.2 Requisitos de ISAKMP

El establecimiento de SA DEBE ser parte del protocolo de manejo de claves definidos para las redes basadas en IP. El concepto de SA es requerido para soportar protocolos de seguridad en ambientes diversos y dinámicos de red. La autentificación y el intercambio de claves deben estar vinculados para asegurar que la clave este establecida con la parte autentificada [DOW92], el establecimiento de una SA debe estar vinculado con la autentificación y el protocolo de intercambio de claves.

ISAKMP proporciona el protocolo de intercambio para establecer una SA entre entidades negociantes después del establecimiento de una SA para estas entidades negociantes en representación de algún protocolo (por ejemplo ESP/AH). Primero, un intercambio inicial de protocolo permite un conjunto de atributos de seguridad acordados. Este conjunto básico proporciona protección para los intercambios subsiguientes de ISAKMP. También indica el método de autentificación y el intercambio de claves que serán realizados como parte del protocolo ISAKMP. Si un conjunto básico de atributos de seguridad ya esta en su sitio entre las entidades de negociación del servidor, el intercambio ISAKMP inicial puede ser omitido y el establecimiento de la SA puede ser realizado directamente. Después de que el conjunto básico de atributos de seguridad haya sido acordado, la autenticidad

de identidad inicial, y las claves requeridas generadas, la SA establecida puede ser usada para comunicaciones subsiguientes por la entidad que invocó a ISAKMP. El conjunto básico de atributos de SA que DEBE ser implementado para proporcionar interoperatibilidad entre ISAKMPs están definidos en el Apéndice A.

1.5 Autentificación

Un paso muy importante en el establecimiento de comunicaciones de red seguras es la autentificación de la entidad en el otro extremo de la comunicación. Muchos mecanismos de autentificación están disponibles. Los mecanismos de autentificación pueden clasificarse dentro de dos categorías: Débiles y fuertes. Enviar claves de texto sin encriptar (texto en claro - cleartext) o otra información de autentificación sin protección en una red es débil, debido a la amenaza de lecturas con sniffer de red. El envío unidireccional de claves hasheadas (a las cuales se les hizo un resumen criptográfico) deficientemente elegidas con baja entropía son también débiles, debido a la amenaza de ataques por fuerza bruta en los mensajes sniffer. Mientras que los passwords pueden ser usados para el establecimiento de identidades, no son considerados en este contexto, debido a declaraciones resientes del Consejo de Arquitectura de Internet [IAB]. Las firmas digitales, tales como el Estándar de Firmas Digitales (DDS: Digital Signature Standard) y las firmas Rivest-Shamir-Adleman (RSA) son claves públicas basadas en fuertes mecanismos de autentificación. Al usar claves públicas para firmas digitales, cada entidad requiere una clave pública y una privada. Los certificados son una parte esencial de los mecanismos de autentificación en una firma digital. Los certificados vinculan la identidad de una entidad específica (ya sea un host, un usuario o una aplicación) a sus claves públicas y posiblemente a otra información de seguridad relacionada tales como privilegios, eliminaciones [clearances] y secciones [compartments]. La autentificación basada en firmas digitales requiere una tercera parte confiable o la creación de autoridades de certificación, la cuál firma y distribuye correctamente los certificados. Para información más detallada sobre firmas digitales, tales como DSS y RSA, y certificados ver [Schneier].

1.5.1 Autoridades de Certificación

Los certificados requieren una infraestructura para la generación, verificación, revocación, administración y distribución. La Autoridad de Registración de Políticas en Internet (IPRA) [RFC-1422] a sido establecida para dirigir esta infraestructura por la IETF. La IPRA certifica las Autoridades de Certificación de Políticas (PCA). Las PCAs controlan a las Autoridades de Certificación (CA) las cuales certifican usuarios y entidades dependientes. El trabajo relacionado con la certificación actual incluye a los Sistemas de Nombres de

Dominio (DNS) y a las Extensiones de Seguridad [DNSSEC] las cuales proporcionan la clave firmada a la entidad en el DNS. El Grupo de Trabajo para la Infraestructura de Clave Pública (PKIX) especifica un perfil para Internet para los certificados X.509. Existen también trabajos realizados en la industria para desarrollar Servicios de Directorios X.500 que podrían proporcionar certificados X.509 a los usuarios. La oficina de correo de USA esta desarrollando una jerarquía de Autoridades de Certificación (CA). El Grupo de Trabajo para la Infraestructura de Clave Pública NIST ha estado desarrollando investigaciones en esta área. La Iniciativa de Seguridad de Sistemas de Información Multinivel (MISSI) del Departamento de Defensa del gobierno de USA (DOD) ha comenzado a desarrollar una infraestructura de certificación para el gobierno de USA. Alternativamente si no existe ninguna infraestructura de clave pública, Los PGP certificados de Red de Confianza (Web of Trust certificates) pueden ser utilizados para proporcionar autentificación y privacidad para el usuario en una comunidad de usuarios que se conocen y confían mutuamente.

1.5.2. Nombramiento de la Entidad

El nombre de la entidad es su identidad y está ligado a su clave pública en los certificados. Las CA DEBEN definir la semántica para el nombramiento de los certificados. Vea UNINETT PCA Policy Statements [Berge] como un ejemplo de como una CA define su política de nombramiento. Cuando se verifica un certificado, el nombre es verificado y ese nombre tendrá significado dentro del dominio de esa CA. Un ejemplo son las extensiones de seguridad de los DNS que hacen los servidores CAs del DNS para las zonas y los nodos a los cuales sirven. Los registros de recursos se proporcionan para las claves públicas y las firmas de esas claves. Los nombres asociados a esas claves son asociados con las direcciones IP y con los nombres de dominio los cuales tienen un significado para las entidades que tienen acceso al DNS para esa información. Una Red de Confianza es otro ejemplo. Cuando se implementan redes de confianza, los nombres están ligados a las claves públicas. En PGP usualmente el nombre de la entidad es usualmente la dirección de e-mail el cuál tiene significado para aquellos, y solamente para aquellos que entienden el correo electrónico. Otra red de confianza podría utilizar un esquema de nombramiento totalmente diferente.

1.5.3 Requerimientos de ISAKMP

La autentificación fuerte DEBE ser proporcionada en los intercambios ISAKMP. Si no se puede autentificar a la entidad del otro extremo, la SA y el establecimiento de claves de sesión serán dudosos. Sin la autentificación no se puede confiar en la identificación de la entidad, lo que hace al control de acceso cuestionable. Mientras que la encriptación (por ejemplo ESP) y la integridad (por ejemplo AH)

protegerán comunicaciones subsiguientes de mirones (sniffer) pasivos, sin autentificación es posible que la SA y las claves hayan sido establecidas por otras personas, las cuales realizaron un ataque activo modificando el flujo de datos trasmitidos interfiriendo la comunicación y ahora se está robando toda su información personal.

Un algoritmo de firma digital DEBE ser usado dentro del componente de autentificación de ISAKMP. Sin embargo, ISAKMP no dictamina un algoritmo para las firmas digitales o Autoridad de Certificación (CA) específico. ISAKMP permite a una entidad iniciar una comunicación indicando que CAs esta utilizando. Después de la selección de una CA, el protocolo proporciona la infraestructura para utilizar el intercambio de autentificación actual. El protocolo proporciona facilidades para la identificación de diferentes autoridades de certificación, tipos de certificados (por ejemplo X.509, PKCS #7, PGP, DNS SIG y registro de claves) y el intercambio de certificados determinados.

ISAKMP utiliza firmas digitales, basadas en criptografía de clave pública, para la autentificación. Existen otros sistemas fuertes de autentificación disponible, que se podrían especificar como mecanismos opcionales de autentificación para ISAKMP. Algunos de estos sistemas de autentificación confían en una tercera parte llamada Centro de Distribución de Claves (KDC), para distribuir claves de sesiones secretas. Un ejemplo es Kerberos, donde la tercera parte confiable es el servidor de Kerberos, que guarda las claves secretas de todos sus clientes y servidores dentro de su dominio de red. Un cliente que tiene una clave secreta proporciona autentificación ante servidores.

Las especificaciones de ISAKMP no especifican el protocolo para la comunicación con las Terceras Partes de Confianza (TTP) o los servicios de directorios de certificados. Estos protocolos están definidos por las TTP y los servicios de directorios y están fuera del alcance de estas especificaciones. El uso de estos servicios adicionales y protocolos serán descriptos en un documento específico de intercambio de claves.

1.6 Criptografía de Clave Pública

La criptografía de clave pública es un modo más flexible, escalable y eficiente para que los usuarios obtengan secretos y claves compartidas para soportar un gran número de formas para ínter-operar con los usuarios de Internet. Muchos algoritmos de generación de claves, que tienen diferentes propiedades, están disponibles para los usuarios (ver [DOW92], [ANSI], y [Oakley]). Las propiedades de los

protocolos de intercambio de claves incluyen un método para el establecimiento de claves, autentificación, simetría, perfect forward secrecy y la protección posterior del tráfico.

NOTA: Las claves criptográficas pueden proteger información por largos periodos de tiempo. Sin embargo esto se basa en la presunción de que las claves son usadas para la protección de comunicaciones y son destruidas después de haber sido usadas y no son almacenadas por ninguna razón.

1.6.1 Propiedades del Intercambio de Claves

Establecimientos de Claves (Generación de Claves/Trasporte de claves): Los dos métodos más comunes de criptografía de clave pública para el establecimiento de claves son, trasporte de claves y generación de claves. Un ejemplo de trasporte de claves es el uso de algoritmos RSA para encriptar una clave de sesión generada aleatoriamente (para encriptar comunicaciones subsiguientes) con los receptores de las claves públicas. La clave aleatoriamente encriptada es luego enviada al receptor, que la desencripta utilizando su clave privada. En este punto ambos extremos de la comunicación, tienen la misma clave de sesión, sin embargo esta fue creada a partir de la entrada de información unidireccional de la comunicación. La ventaja del método de trasporte de claves es que tiene menos gasto computacional que el siguiente método. El algoritmo de Diffie-Hellman (D-H) ilustra la generación de claves utilizando criptografía de clave pública. El algoritmo D-H se inicia con dos usuarios que intercambian información pública. Cada usuario después combina matemáticamente la información pública del otro usuario con su propia información secreta para calcular un valor secreto compartido. Este valor secreto puede ser utilizado como una clave de sesión o como una clave de encriptación de clave para encriptar la clave de sesión generada aleatoriamente. Este método genera una clave de sesión basada en información pública y secreta, compartida por ambos usuarios. La ventaja del algoritmo de D-H es que la clave usada para encriptar mensajes se obtiene de la información compartida por ambos usuarios y la independencia de las claves entre un intercambio de claves y el otro proporciona perfect forward secrecy. Descripciones detalladas de estos algoritmos pueden ser encontradas en [Schneier]. Hay varias versiones de estos dos esquemas de generación de claves pero estas versiones no necesariamente deben interrelacionarse.

Autentificación del intercambio de claves: Los intercambios de claves pueden ser autentificados durante el protocolo o después del protocolo. La autentificación del intercambio de claves durante el protocolo se lleva a cabo cuando cada parte proporciona prueba de que tiene la clave de sesión secreta antes de finalizar el protocolo. La prueba puede ser proporcionada encriptando datos conocidos en la

sesión de claves secretas durante el intercambio del protocolo. La autentificación después del protocolo debe ocurrir en comunicaciones subsiguientes. La autentificación durante el protocolo es la que se prefiere. Por lo tanto las comunicaciones subsiguientes no son iniciadas si la clave de sesión secreta no esta establecida con la parte deseada.

Intercambio de claves simétrico: un intercambio de claves proporciona simetría si cualquier parte puede iniciar el intercambio y los mensajes intercambiados pueden cruzarse en la trayectoria sin afectar la clave que es generada. Esto es provechoso para que el cálculo de claves no requiera que cada parte sepa quien inició el intercambio. A pesar de que el intercambio de claves simétricos es provechoso, la simetría en el protocolo de administración de claves puede proporcionar vulnerabilidad a los ataques de reflexión (reflection attacks).

Perfect Forward Secrecy: según lo descripto en [DOW92], un protocolo de intercambio de claves autentificado, proporciona perfect forward secrecy si la divulgación del material clave por largo tiempo no compromete la confidencialidad del intercambio de claves de las comunicaciones previas. Las características del perfect forward secrecy no se aplican al intercambio de claves cuando este está desprovisto de

1.6.2 Requisitos para ISAKMP

Un intercambio de claves autentificado debe ser utilizado por ISAKMP. Los usuarios DEBERÍAN elegir los algoritmos de establecimiento de claves adicionales basándose en sus propios requerimientos. ISAKMP no especifica un intercambio de claves determinado. Sin embargo, [IKE] describe una propuesta para el uso de [Oakley] en conjunto con ISAKMP. Los requerimientos que deben ser evaluados al elegir un algoritmo de establecimiento de claves deben incluir el método de establecimiento (generación o trasporte), perfect forward secrecy, el costo computacional, depósito de claves, y robustez de las claves. De acuerdo con los requerimientos del usuario, ISAKMP permite a una entidad iniciar comunicaciones para que indique que intercambio de claves soporta. Después de la selección de un intercambio de claves el protocolo proporciona los mensajes requeridos para soportar el establecimiento de la verdadera clave.

1.7 Protección ISAKMP

1.7.1 Anti-Saturación (Denegación de Servicio)

De los numerosos servicios de seguridad disponibles, la protección contra la denegación de servicio siempre va ha ser uno de los más

difíciles de tratar. Un "cookie" o token anti-saturación (ACT) está destinado a la protección de recursos computacionales de ataques sin malgastar recursos excesivos de CPU, para determinar sus autenticidades. Un intercambio previo con operaciones de claves públicas que consuman mucha CPU pueden frustrar ciertas tentativas de denegación de servicios (por ejemplo, con inundaciones de falsas direcciones IP de origen). La protección absoluta contra la denegación de servicio es imposible pero este token anti-saturación proporciona una técnica para hacerlo más fácil de manejar. El uso del token anti-saturación fue introducido por Karn y Simplón en [Karn].

Como se observará en los intercambios mostrados en la sección 4, los mecanismos de anti-saturación deberían ser usados en conjunto con mecanismos de recolección de información de estado no válida; un atacante silencioso puede inundar un servidor usando paquetes con direcciones IP falsas y se creará la causa producida. Tales técnicas de administración de memoria agresiva DEBERÍAN ser empleados por los protocolos que utilizan ISAKMP, que no realizan un minucioso examen inicial, solo en la fase de anti-saturación, como se describe en [Karn].

1.7.2 Secuestro de la Conexión

ISAKMP previene el secuestro de la conexión vinculando la autentificación, el intercambio de claves y el intercambio de SAs. Esta vinculación impide a un atacante completar la autentificación y que luego intervenga y tome la personalidad de una entidad durante los intercambios de claves y SA.

1.7.3 Ataques en la Trayectoria (Man-in-the-Middle Attacks)

La intercepción de atacantes en la trayectoria (Man-in-the-Middle Attacks) incluyen: la intercepción, la inserción, la cancelación y la modificación de mensajes, mensajes reflejados por atrás del emisor reeditando mensajes viejos y redireccionando mensajes. Las características de ISAKMP evitan que estos tipos de ataques sean exitosos. La vinculación de intercambios ISAKMP previene la inserción de mensajes en el intercambio de los protocolos. La máquina de estado del protocolo ISAKMP se define como un eliminador de mensajes, que no permite que SA parciales sean creadas, la máquina de estado eliminará todos los estados y volverá a la inactividad. La máquina de estado también evita que la reflexión de un mensaje cause daños. Los requerimientos para una nueva cookie con contenido dinámico para cada nueva SA establecida previene de ataques que involucren el reenvío de mensajes viejos. El requerimiento de autentificación fuerte de ISAKMP previene que una SA sea establecida con cualquier otra parte que no sea la deseada. Los mensajes pueden ser redireccionados a un destino diferente o modificados pero esto será detectado y una SA no será

establecida. La especificación de ISAKMP define donde a ocurrido un procesamiento anormal y recomienda notificar a la parte apropiada de esta anormalidad.

1.8 Comunicaciones Multicast

Se espera que las comunicaciones multicast requieran de los mismos servicios de seguridad que las comunicaciones unicast y pueden introducir la necesidad de servicios de seguridad adicionales. Los asuntos para la distribución de SPIs para el tráfico multicast son presentadas en [SEC-ARCH]. Los temas de multicast también son debatidos en [RFC-1949] y en [BC]. Una extensión futura para ISAKMP soportará la distribución de claves multicast. Para una introducción en estos temas relacionados con la seguridad multicast, consulte los Drafts de Internet, [RFC-2094] y [RFC-2093], que describiendo la investigación de Sparta's en esta área.

2. Conceptos y Terminologías

2.1 Terminología de ISAKMP

Protocolo de Seguridad: Un Protocolo de Seguridad consiste en una entidad de un solo extremo en la pila de red, realizando un servicio de seguridad para las comunicaciones de red. Por ejemplo, ESP IPsec, AH IPsec, son dos diferentes protocolos de seguridad. TLS es otro ejemplo. Los protocolos de seguridad pueden proporcionar más de un servicio, por ejemplo proporcionar integrabilidad y confidencialidad en un solo módulo.

Conjunto de Protección: Un conjunto de protección es una lista de servicios de seguridad que debe ser aplicada por varios protocolos de seguridad. Por ejemplo, un conjunto de protección puede consistir de encriptación DES en ESP IP, y una clave MD5 en AH IP. Todas las protecciones en un conjunto deben ser tratadas como una unidad simple. Esto es necesario porque los servicios de seguridad en diferentes protocolos de seguridad pueden tener sutiles interaccionés, y los efectos de un conjunto deben ser analizados y verificados como un todo.

Asociación de seguridad (SA): Una Asociación de seguridad es un conjunto de parámetros específicos del protocolo de seguridad que definen completamente los servicios y mecanismos necesarios para proteger el tráfico en ese lugar del protocolo de seguridad. Estos parámetros pueden incluir identificadores de algoritmo, modos, claves criptográficas, etc. La SA hace referencia a su protocolo de seguridad asociado (por ejemplo "SA ISAKMP", "SA ESP", "SA TLS").

SA ISAKMP: Una SA usada por los servidores ISAKMP para proteger su propio tráfico. Las Secciones 2.3 y 2.4 proporcionan más detalles acerca de las SAs ISAKMP.

Índice de parámetros de seguridad (SPI): Un identificador para una Asociación de Seguridad, relativo a algún protocolo de seguridad. Cada protocolo de seguridad tiene su propio "espacio-SPI". Un par (protocolo de seguridad, SPI) pueden identificar unívocamente a una SA. La unívocariedad (exclusividad) de la SPI es dependiente de la implementación, pero puede estar basada en sistemas, en protocolos, u otras opciones. Dependiendo del DOI, información adicional (por ejemplo, las direcciones de los host) puede ser necesarias para identificar a una SA. El DOI también determinará cuales SPIs (es decir, los SPIs del iniciador o del respondedor) son enviados durante la comunicación.

Dominio de Interpretación (DOI): Un Dominio de Interpretación (DOI) define los formatos de cargas, tipos de intercambio, y convenciones para nombrar información relevante a la seguridad tales como políticas de seguridad o algoritmos criptográficos y modos. Un identificador de Dominio de Interpretación (DOI) es usado para interpretar las cargas de las cargas ISAKMP. Un sistema DEBERÍA soportar múltiples Dominios de Interpretación simultáneamente. El concepto de DOI se basa en trabajos previos del Grupo de Trabajo de TSIG CIPSO, pero se extiende más allá de la interpretación de etiquetas de seguridad para incluir el nombramiento y la interpretación de los servicios de seguridad. Un DOI define:

- Una "situación": el conjunto de información que será usado para determinar los servicios de seguridad requeridos.
- El conjunto de políticas de seguridad que deben o podrían ser soportados.
- La sintaxis para la especificación de los propósitos de los servicios de seguridad sugeridos.
- Un esquema para nombrar información relativa a la seguridad, incluyendo algoritmos de encriptación, algoritmos de intercambio de claves, atributos de política de seguridad y autoridades de certificación.
- Los formatos específicos de los contenidos de las diversas cargas.
- Tipos de intercambio adicionales, si son requeridos.

Las reglas de Seguridad DOI IP IETF se presentan en [IPDOI]. Las especificaciones de las reglas para DOI personalizados serán presentadas en documentos separados.

Situación: Una situación contiene toda la información relevante a la seguridad que un sistema considera necesaria para decidir los servicios de seguridad requeridos para proteger las sesiones que están siendo negociadas. La situación puede incluir direcciones, clasificaciones de seguridad, modos de operación, (normal vs. emergencia), etc.

Proposición: una proposición es una lista, en orden decreciente de preferencia, del conjunto de protecciones que un sistema considera aceptable para proteger el tráfico bajo una situación dada.

Carga: ISAKMP define varios tipos de cargas, que son usadas para trasmitir información según los datos de la SA, o los datos del intercambio de claves, dentro de las formas definidas en el DOI. Una carga consiste en una cabecera de carga genérica y en octetos encadenados que están ocultos para ISAKMP. ISAKMP usa funcionalidades específicas del DOI para sintetizar e interpretar esas cargas. Múltiples cargas pueden ser enviadas en un único mensaje de ISAKMP. Ver la Sección 3 para más detalles de tipos de carga, y [IPDOI] para los formatos de seguridad de cargas DOI IP IETF.

Tipos de Intercambios: Un tipo de intercambio es una especificación de un número de mensajes en un intercambio ISAKMP, y los tipos de carga que están contenidos en cada uno de estos mensajes. Cada tipo de intercambio está diseñado para proporcionar, un conjunto especifico de servicios de seguridad, tales como el anonimato de los participantes, perfect forward secrecy del material clave, autentificación para los participantes, etc. En la Sección 4.1 se define el conjunto por defecto de tipos de intercambio ISAKMP. Otros tipos de intercambio se pueden agregar para soportar intercambios adicionales de claves, si es requerido.

2.2 Ubicación de ISAKMP

La Figura 1 es una vista de la ubicación de ISAKMP dentro de un contexto de un sistema en una arquitectura de red. Una parte importante de la negociación de los servicios de red es considerar a la "PILA" entera de las SAs como una unidad. Esto se lo denomina "conjunto de protección".

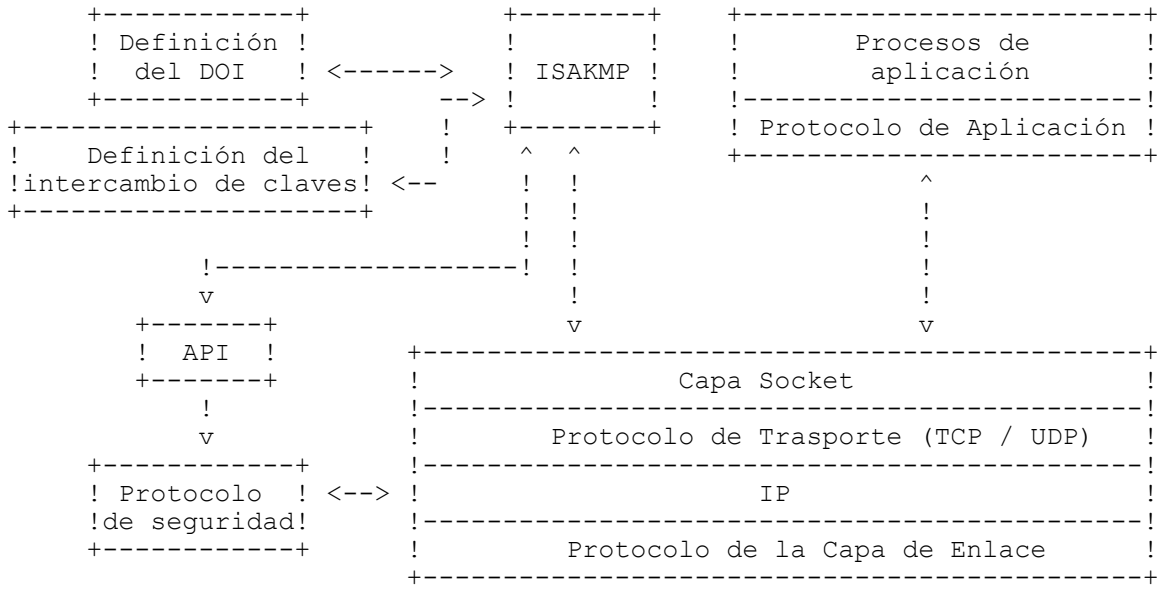


Figura 1: Ubicación de ISAKMP

2.3 Fases de la Negociación

ISAKMP ofrece dos "fases" para la negociación. En la primera fase, dos entidades (por ejemplo, servidores ISAKMP) concuerdan en como proteger futuras negociaciones del tráfico entre ellas mismas, estableciendo una SA ISAKMP. Esta SA ISAKMP es luego usada para proteger las negociaciones requeridas por las SA de los Protocolos. Dos entidades (por ejemplo, servidores de ISAKMP) pueden negociar (si están activos) múltiples SA ISAKMP.

La segunda fase de la negociación es usada para establecer la SA para otros protocolos de seguridad. Esta segunda fase puede ser usada para establecer múltiples SA. Las SA establecidas por ISAKMP durante esta fase pueden ser usadas por un protocolo de seguridad para proteger los intercambios de datos/mensajes.

Mientras que este método de dos fases tiene un costo elevado para la inicialización en la mayoría de los escenarios simples, hay varias razones por la que este método es beneficioso en la mayoría de los casos.

Primero, las entidades (por ejemplo servidores ISAKMP) pueden amortizar el costo de la primera fase a través de varias negociaciones en la segunda fase. Esto permite que múltiples SAs

estén relacionadas entre usuarios por un cierto lapso de tiempo sin tener que iniciar cada una de las comunicaciones.

Segundo, los servicios de seguridad negociados durante la primer fase proporcionan propiedades de seguridad para la segunda fase. Por ejemplo, después de la negociación de la primera fase, la encriptación proporcionada por la SA ISAKMP puede proporcionar protección de identidad, potencialmente permitiendo el uso de intercambios más simples, en la segunda fase. Por otra parte, si un canal establecido durante la primera fase no es adecuado para proteger las identidades, la segunda fase luego deberá negociar los mecanismos de seguridad adecuados.

Tercero, tener una SA ISAKMP reduce considerablemente el costo de actividad de administración externo a ISAKMP brindando una "trayectoria confiable" para una SA ISAKMP, las entidades (por ejemplo servidores de ISAKMP) tendrían que pasar por una reautorización completa de cada error de notificación o la cancelación de una SA.

La negociación llevada a cabo en cada fase es realizada usando intercambios ISAKMP definidos (ver Sección 4) o intercambios definíos en un intercambio de claves dentro de un DOI.

Note que los servicios de seguridad se pueden aplicar de manera diferente en cada una de las fases de la negociación. Por ejemplo, diferentes partes son autentificadas durante cada una de las fases de la negociación. Durante la primera fase, las partes que son autentificadas pueden ser servidores ISAKMP o host, mientras que en la segunda fase usuarios o programas de nivel de aplicación son autentificados.

2.4 Identificar SA

A pesar de que existen canales seguros de bootstrapping entre sistemas, ISAKMP no puede asumir la existencia de servicios de seguridad, y debe proporcionar algunas protecciones para sí mismo. Por lo tanto, ISAKMP considera una SA ISAKMP diferente a las de otros tipos y administra las SA ISAKMP para sí mismo, con su propio espacio de nombres. ISAKMP usa dos campos de cookies en la cabecera de ISAKMP para identificar SA ISAKMP. El Identificador (ID) de mensaje en la Cabecera de ISAKMP y el campo SPI en la carga de la Propuesta son usados durante el establecimiento de la SA para identificar la SA de otros protocolos de seguridad. La interpretación de estos 4 campos es dependiente de la operación que se lleve a cabo.

La tabla siguiente muestra la presencia o ausencia de diversos campos durante el establecimiento de la SA. Los siguientes campos son necesarios para las diversas operaciones asociadas con el establecimiento de la SA: cookies en la cabecera de ISAKMP, el campo ID (identificador) de mensaje en la cabecera de ISAKMP, y el campo SPI en la carga de la Propuesta. Una 'X' en la columna significa que el valor debe estar presente. Una 'NA' en la columna significa que el valor en la columna no es aplicable en esa operación.

#	Operación	Cookie del Iniciador	Cookie del Respondedor	ID del Mensaje	SPI
(1)	Inicio de la negociación SA ISAKMP	X	0	0	0
(2)	El respondedor de la negociación SA ISAKMP	X	X	0	0
(3)	Iniciador, negociación de la otra SA	X	X	X	X
(4)	El respondedor, negociación de otra SA	X	X	X	X
(5)	Otros (KE, ID, etc.)	X	X	X/0	NA
(6)	Protocolo de Seguridad (AH, ESP)	NA	NA	NA	X

En la primera línea (1) de la tabla, el iniciador incluye el campo del Cookie del Iniciador en la cabecera de ISAKMP usando los procedimientos descriptos en las Secciones 2.5.3 y 3.1.

En la segunda línea (2) de la tabla, el respondedor incluye los campos de las cookies del iniciador y del respondedor en la cabecera de ISAKMP usando los procedimientos descriptos en las Secciones 2.5.3 y 3.1. Mensajes adicionales pueden ser intercambiados entre usuarios ISAKMP, dependiendo del primer tipo de intercambio ISAKMP utilizado durante la primera fase de la negociación. Una vez que la primera fase del intercambio a finalizado, las cookies del iniciador y del respondedor son incluidos en la cabecera de ISAKMP para todas las comunicaciones subsiguientes entre los usuarios de ISAKMP.

Durante la fase 1 de la negociación, la cookie del iniciador y del respondedor determinan la SA ISAKMP. Por lo tanto el campo SPI en la carga de la Propuesta es redundante y PUEDE cero (0) o PUEDE contener la identidad del cookie del transmisor.

En la tercera línea (3) de la tabla, el iniciador asocia el ID (identificador) del Mensaje con los Protocolos contenidos en la Propuesta SA. Este ID (identificador) de Mensaje y los SPI del iniciador asociados con cada protocolo en la Propuesta son enviados al respondedor. Los SPI(s) serán utilizados por los protocolos de seguridad una vez que la fase 2 de la negociación este terminada.

En la cuarta línea (4) de la tabla, el que responde incluye el mismo Identificador de Mensaje y los mismos SPI(s) que están asociados con cada protocolo en la Propuesta aceptada. Esta información se devuelve al iniciador.

En la quinta línea (5) de la tabla, el iniciador y el que responde usan el campo de ID (identificador) de Mensaje en la cabecera de ISAKMP para mantener el camino de la negociación del protocolo en proceso. Esto es solo aplicable para el intercambio de la fase 2 y el valor DEBE ser cero para el intercambio en la fase 1 por que las cookies combinadas identifican la SA ISAKMP. El campo SPI en la carga de la Propuesta no es aplicable por que la carga de la Propuesta es solamente usada durante los intercambios de negociación de mensajes de SA (pasos 3 y 4).

En la secta línea (6) de la tabla, la fase 2 de la negociación es terminada. Los protocolos de seguridad usan los SPI(s) para determinar que mecanismos y servicios de seguridad aplicar a la comunicación entre ellos. El valor del SPI mostrado en la secta línea no es el campo SPI de la carga de la Propuesta sino que es el campo del SPI contenido dentro de la cabecera del protocolo de seguridad.

Durante el establecimiento de la SA, una SPI debe ser generada. ISAKMP esta diseñado para tratar con SPIs de diferentes tamaños, esto se logra usando campos con tamaños de SPIs dentro de la carga de la Propuesta durante el establecimiento de la SA. El manejo de los SPIs será detallado por la especificación de DOI (por ejemplo [IPDOI]).

Cuando una SA es inicialmente establecida, uno de los extremos asume el rol de iniciador y el otro el rol de respondedor. Una vez que la SA esta establecida, ambos el iniciador original y el respondedor original pueden iniciar la fase 2 de la negociación como entidades pares (peer entity). Por ende, las SA ISAKMP son bidireccionales por naturaleza.

Además, ISAKMP permite al iniciador y al respondedor tener el mismo control durante el proceso de negociación. Mientras que ISAKMP es configurada para permitir la negociación de una SA que incluye múltiples propuestas, el iniciador puede mantener cierto control haciendo solamente una propuesta de acuerdo con la política de seguridad local del iniciador. Una vez que el iniciador envía una propuesta que contiene más de una propuesta (que son enviadas en orden decreciente de preferencia), el iniciador le pasa el control al respondedor. Una vez que el respondedor esta en control del establecimiento de la SA puede hacer que sus políticas tomen precedencia sobre las del iniciador dentro de un contexto de opciones

múltiples ofrecidas por el iniciador. Esto se logra seleccionando la mejor propuesta adecuada para la política de seguridad local del respondedor y devolviendo esta selección al iniciador.

2.5 Temas Diversos

2.5.1 Protocolo de trasporte

ISAKMP puede ser implementado sobre cualquier protocolo de trasporte o sobre el mismo IP. Las implementaciones DEBEN incluir la capacidad de enviar y recibir tráfico ISAKMP utilizando el Protocolo de Datagrama de Usuario (UDP) sobre el puerto 500. El puerto UDP 500 ha sido asignado para el tráfico de ISAKMP por la Autoridad de Asignación de Números en Internet (IANA). Implementaciones adicionales PUEDEN soportar otros protocolos de trasporte o sobre el mismo protocolo IP.

2.5.2 Campos RESERVADOS

La existencia de campos RESERVADOS dentro de la carga ISAKMP son usados estrictamente para preservar el alineamiento de los bytes. Todos los campos RESERVADOS en el protocolo ISAKMP DEBEN contener el valor cero (0) cuando un paquete es enviado. El receptor DEBERÍA corroborar que los campos RESERVADOS contengan el valor cero (0) y descartar el paquete si otros valores son encontrados

2.5.3 Creación de Token ("Cookies") Anti-Saturación

Los detalles de la generación de cookies dependen de la implementación, pero DEBEN satisfacer estos requerimientos básicos (originariamente declarados por Phil Karn en [Karn]):

1. La cookie debe depender de las partes específicas. Esto evita que un atacante obtenga una cookie usando una dirección IP real y un puerto UDP, y luego use esto para saturar a la victima con peticiones de Diffie-Hellman a partir de direcciones IP o puertos elegidos aleatoriamente.

2. No debe ser posible que cualquier persona con excepción de la entidad emita la generación de cookies que serán aceptadas por esa entidad. Esto implica que la entidad emisora debe utilizar información local secreta en la generación y en las subsiguientes verificaciones de cookies. No debe ser posible deducir esta información secreta de ninguna cookie en particular.

3. La función de generación de cookies debe ser rápida para impedir ataques que intentan sabotear los recursos de la CPU.

El método sugerido por Karn's para la creación de cookies es realizar un hash (por ejemplo MD5) sobre la dirección de origen y destino IP, la dirección de los puertos de origen y de destino UDP y un valor secreto aleatorio generado localmente. ISAKMP requiere que la cookie sea única para cada SA establecida con el propósito de ayudar a prevenir ataques de reenvío, por lo tanto, la fecha y el tiempo DEBEN ser agregados a la información condensada (hashed). Las cookies generadas son colocadas en los campos de las cookies del Iniciador y del Respondedor de la Cabecera ISAKMP (como se describe en la Sección 3.1). Estos campos tienen una longitud de 8 octetos, por ende se requiere que la cookie generada tenga 8 octetos. Los mensajes de Notificación y Cancelación (ver las Secciones 3.14, 3.15 y 4.8) unidireccionalmente trasmitidos y que están bajo la protección de una SA ISAKMP existente, no requerirán la generación de una nueva cookie. Una excepción a esto es la transmisión de un Mensaje de Notificación durante el intercambio de la fase 1, antes de terminar el establecimiento de una SA. Las Secciones 3.14 y 4.8 proporcionan detalles adicionales.

3 Cargas de ISAKMP

Las cargas de ISAKMP proporcionan bloques modulares para la construcción de mensajes ISAKMP. La presencia y el ordenamiento de las cargas ISAKMP se define y depende del Campo Tipo de Intercambio ubicado en la Cabecera de ISAKMP (ver figura 2). Los tipos de carga de ISAKMP son analizados desde la Sección 3.4 hasta la Sección 3.15. Las descripciones de las cargas de ISAKMP, de los mensajes e intercambios se muestran usando el ordenamiento de octetos de red.

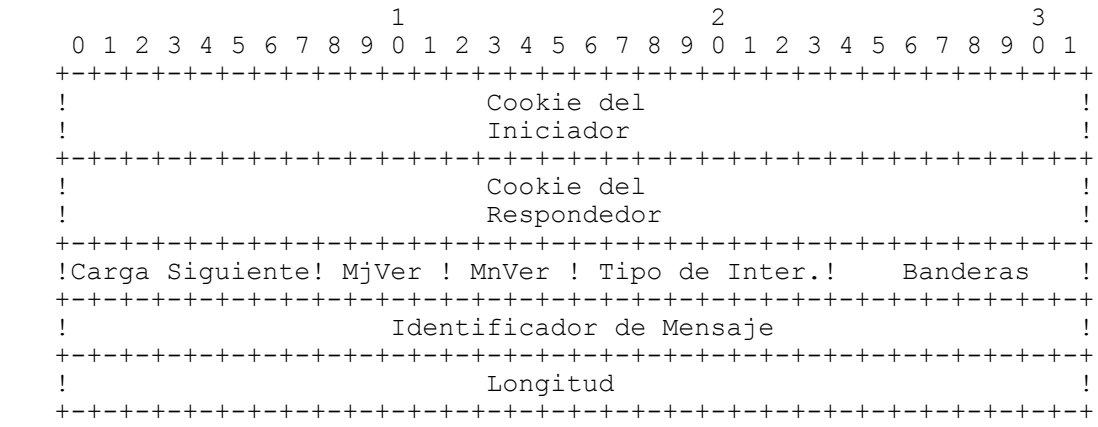
3.1 Formato de la Cabecera de ISAKMP

El mensaje de ISAKMP tiene un formato de cabecera fijo, como muestra la figura 2, seguido por un número de cargas variables. Una cabecera fija simplifica el procesamiento, proporcionando el beneficio del análisis de procesamiento del software del Protocolo que es menos complejo y mas fácil de implementar. La cabecera fija contiene la información requerida por el protocolo para mantener el estado, procesar las cargas y posiblemente prevenir la denegación de servicio o ataques de reenvío.

Los campos de la Cabecera ISAKMP se definen de la siguiente forma:

- Cookie del Iniciador (8 octetos): Cookie de la entidad que responde al requerimiento del establecimiento de una SA, o cancelación de la SA.

- Cookie del Respondedor (8 octetos): Cookie de la entidad que responde al requerimiento del establecimiento de una SA, o cancelación de una SA.



MjVer = Versión mayor; MnVer = Versión menor

Figura 2: Formato de la Cabecera ISAKMP

- Carga siguiente (1 octeto): indica el tipo de carga en el primer mensaje el formato de cada carga es definido desde la sección 3.4 hasta la sección 3.16. El procesamiento para las cargas se define en la sección 5.

Tipos de carga siguiente	Valor
Ninguno	0
Asociación de Seguridad (SA)	1
Propuesta (P)	2
Transformación (T)	3
Intercambio de claves (KE)	4
Identificación (ID)	5
Certificado (CERT)	6
Solicitud de certificado (CR)	7
Hash (HASH)	8
Firma (SIG)	9
Nonce (NONCE)	10
Notificación (N)	11
Cancelación (D)	12
Identificación del vendedor (VID)	13
RESERVADO	14-127
Uso privado	128-255

- Versión Mayor (4 bits): indica la versión mayor del protocolo ISAKMP en uso. Las implementaciones basadas en esta versión de Draft-Internet de ISAKMP DEBEN fijar la versión mayor en uno. Las implementación basadas en versiones previas de Draft-Internet de ISAKMP deben fijar la versión mayor en 0. Las implementaciones nunca DEBERÍAN aceptar paquetes con un número de versión mayor que estos.

- Versión Menor (4 bits): indica la versión menor del protocolo ISAKMP en uso. Las implementaciones basadas en los Draft-Internet de ISAKMP DEBEN fijar la versión menor en cero. Las implementaciones basadas en versiones previas de los Draft-Internet de ISAKMP deben fijar la versión menor en 1. Las implementaciones nunca DEBERÍAN aceptar paquetes con un número de versión superior a estos, dado que los números de la versión mayor son idénticos.

- Tipo de intercambio (1 octeto): Indica el tipo de intercambio que esta siendo usado. Esto indica los ordenamientos de los mensajes y la carga en los intercambios de ISAKMP.

Tipos de Intercambios	Valor
Ninguno	0
Base	1
Protección de Identidad	2
Solamente Autentificación	3
Agresivo	4
Informativo	5
Uso futuro de ISAKMP	6-31
Uso especifico del DOI	32-239
Uso privado	240-255

- o Banderas (Flags) (1 octeto): Indica las opciones específicas que se fijan para los intercambios ISAKMP. Las banderas enumeradas debajo son específicas del campo de Banderas comenzando con el bit menos significativo, es decir el bit de Encriptación es el que se encuentra en la posición cero en el campo de Banderas, el bit de Commit está en la posición 1 en el campo de Banderas, y el bit de Solo Autentificación en la posición 2 del campo de Banderas. Los bits restantes del campo de Banderas se BEBEN fijar en cero antes de la transmisión.

  - -- Bit de Encriptación (1 bit): si está en 1, todas las cargas que siguen a la cabecera son encriptadas usando algoritmos de encriptación, identificados por la SA ISAKMP. El identificador de la SA ISAKMP es la combinación de la cookie del iniciador y del respondedor. Se RECOMIENDA que la encriptación de las comunicaciones se realicen lo antes posible entre los usuarios. Para todos los intercambios ISAKMP descriptos en la Sección 4.1, la encriptación DEBERÍA comenzar después de que ambas partes hallan intercambiado las cargas de Intercambio de Claves. Si el Bit de encriptación no está en cero (0) las cargas no son encriptadas.

  - -- Bit de Commit (1 bit): Este bit es usado para señalar la sincronización del intercambio de claves. Es usado para asegurar que el material encriptado no se reciba antes del término del establecimiento de la SA. EL bit de Commit puede ser fijado (en cualquier momento) por cualquiera de las partes que participan en el establecimiento de la SA, y puede ser usado durante las dos fases del establecimiento de la SA ISAKMP. Sin embargo, el valor DEBE ser puesto en cero (resetiado) después de la fase 1 de la negociación. Si está en (1), la entidad que no lo haya fijado DEBE esperar un Intercambio Informativo conteniendo una carga de Notificación (con el Mensaje de Notificación CONECTADO) de la entidad que fijó el Bit de Commit. En este caso, el campo Identificador de Mensaje del Intercambio Informativo DEBE contener el Identificador de Mensaje de la ISAKMP original de la fase 2 de

negociación de la SA. Esto se hace para asegurar que el Intercambio Informativo con el Mensaje de Notificación CONECTADO pueda ser asociado con la correcta fase dos de la SA. La recepción y procesamiento del Intercambio Informativo indica que el establecimiento de la SA fue exitoso y que cualquier entidad puede ahora proceder con la comunicación del tráfico encriptado. En sincronizaciones adicionales del intercambio de claves, el Bit de Commit puede ser usado para proteger contra la pérdida de trasmisiones en redes no confiables y para la defensa de múltiples retrasmisiones.

NOTA: Es siempre posible que el mensaje final de un intercambio se pueda perder. En este caso, la entidad que se prepara para recibir el mensaje final de un intercambio recibiría el mensaje de la negociación de la fase 2 de la SA seguido de un intercambio de la fase 1 o el tráfico encriptado seguido de un intercambio de la fase 2. El manejo de esta situación no está estandarizado, pero proponemos las siguientes posibilidades. Si la entidad que espera el Intercambio Informativo puede verificar el mensaje recibido (es decir, el mensaje de negociación de la fase 2 de la SA o el tráfico encriptado), entonces PUEDE considerarse que la SA fue establecida y continuar con el procesamiento. Otra opción es retrasmitir el último mensaje ISAKMP para forzar a la otra entidad a retrasmitir el mensaje final. Esto sugiere que las implementaciones pueden considerar la retención del último mensaje (localmente) hasta que estén seguras de que la SA está establecida.

-- Bit de Solo Autentificación (1 bit): este bit esta diseñado para ser usado con el Intercambio Informativo de una carga de Notificación y permitirá la transmisión de información con comprobación de integridad, pero no de encriptación (por ejemplo en modo de emergencia). La sección 4.8 indica que un Intercambio Informativo de la fase 2 DEBE ser enviado bajo la protección de una SA ISAKMP. Esto es solo una excepción a esa política. Si el bit de Solo Autentificación está en (1), solamente los servicios de autentificación de seguridad serán aplicados a toda la carga de Notificación de Intercambio Informativo y la carga no será encriptada.

o Identificador (ID) de Mensaje (4 octetos): El Identificador de Mensaje solamente se usa para identificar el protocolo durante las negociaciones de la fase 2. Este valor es generado aleatoriamente por el iniciador de la fase 2. En el caso de establecimientos simultáneos de SA (es decir colisiones), el valor de este campo será probablemente diferente porque son generados independientemente y, así, dos SAs seguirán con el

establecimiento. Sin embargo es improbable de que existan establecimientos simultáneos. Durante las negociaciones de la fase 1, el valor DEBE ser cero.

- Longitud (4 octetos): Longitud total del mensaje (cabecera más cargas) en octetos. La encriptación puede expandir el tamaño de un mensaje ISAKMP.

3.2 Cabecera de Carga Genérica

Cada carga ISAKMP definidas desde la Sección 3.4 hasta la Sección 3.16 comienzan con una cabecera genérica, como se muestra en la Figura 3, la cual proporciona una capacidad de encadenamiento de carga y claramente define los límites de una carga.

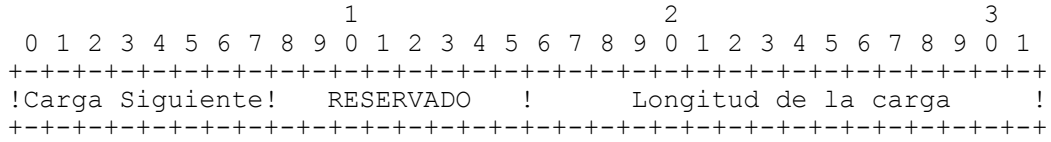


Figura 3: Formato de la Cabecera de Carga Genérica

Los campos de la cabecera de la carga genérica son definidos de la siguiente forma:

- Carga Siguiente (1 octeto): Identificador del tipo de carga de la siguiente carga en el mensaje. Si la carga actual es la última en el mensaje, este campo contendrá el valor cero. Este campo proporciona la capacidad de "encadenamiento".

- RESERVADO (1 octeto): No utilizado, debe contener ceros.

- Longitud de la carga (2 octetos): Longitud de la carga actual en octetos, incluyendo la cabecera de carga genérica.

3.3 Atributos de los Datos

Hay varios casos dentro de ISAKMP donde es necesario representar los Atributos de los Datos. Un ejemplo de esto es los Atributos de la SA contenidas en la carga de Transformación (descriptos en la Sección 3.6). Estos Atributos de los Datos no son carga ISAKMP, pero están contenidos dentro de las cargas de ISAKMP. El formato de los Atributos de los Datos proporciona la flexibilidad para la representación de diferentes tipos de información. Pueden existir múltiples Atributos de los Datos dentro de una carga. La longitud de los atributos de los datos será de 4 octetos o estará definida por el campo Longitud de los Atributos. Esto es realizado usando el bit de

Formato de los Atributo descriptos debajo. La información específica acerca de los atributos para cada dominio será descripta en un documento DOI, por ejemplo, DOI IPsec [IPDOI].

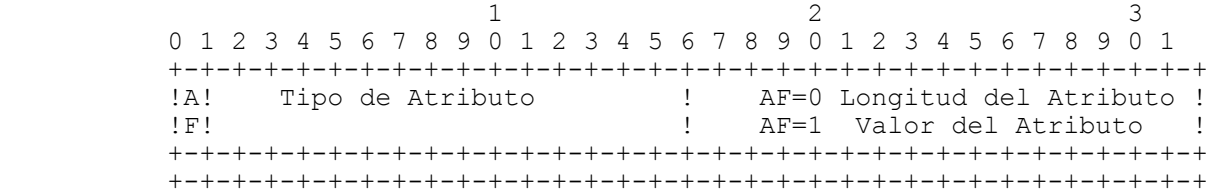


Figura 4: Formato de los Atributo de los Datos

Los campos de los Atributos de los Datos se definen de la siguiente forma:

- Tipo de Atributo (2 octetos): identificador único para cada tipo de Atributo. Estos atributos se definen como parte de la información especifica del DOI.

  El bits más significativo, o Formato de Atributo (AF), indica si los atributos de los datos siguen el formato de Tipo/Longitud/valor (TLV) o uno más corto que sería; Tipo/valor (TV). Si el AF es cero (0), entonces los atributos de los datos tienen el formato Tipo/Longitud/valor (TLV). Si el bit AF es uno (1), entonces los Atributos de los Datos tienen el formato Tipo/Valor.

- Longitud del Atributo (2 octetos): La longitud en octetos del Valor del Atributo. Cuando el bit AF está en uno (1), el Valor del Atributo es solamente de 2 octetos y el campo Longitud del Atributo no está presente.

- Valor del Atributo (longitud variable): Valor del Atributo asociado con el Tipo de Atributo especifico del DOI. Si el bit AF esta en cero (0), este campo tiene una longitud variable determinada por el campo de Longitud del Atributo. Si el bit AF está en uno (1), el Valor del Atributo tiene una longitud de 2 octetos.

3.4 Carga SA

La carga SA es usada para negociar los atributos de seguridad y para indicar el Dominio de Interpretación (DOI) y la situación bajo la cual esta tomando lugar. La Figura 5 muestra el formato de la carga SA.

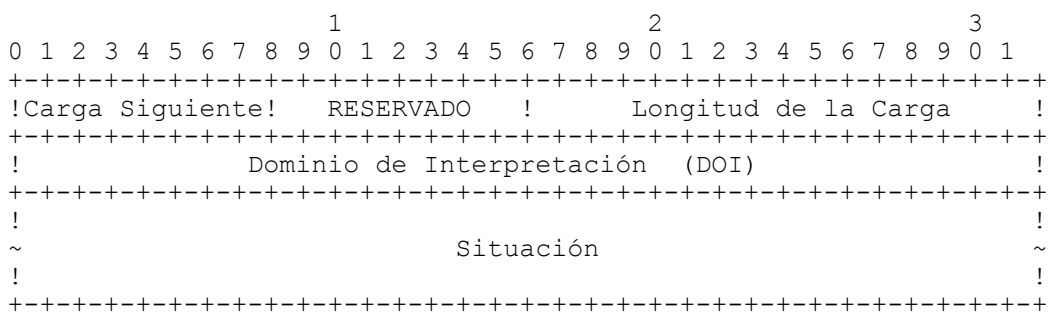


Figura 5: Formato de la carga SA

- Carga Siguiente (1 octeto): identificador del tipo de carga de la siguiente carga en el mensaje. Si la carga actual es la última en el mensaje este campo contendrá el valor cero (0). Este campo NO DEBE contener los valores de las cargas de la Propuesta o Transformación ya que estas son consideradas parte de la negociación de la SA. Por ejemplo, este campo contendría el valor "10" (carga Nonce), en el primer mensaje de un Intercambio Base (ver Sección 4.4) y el valor "0" en el primer mensaje en un Intercambio de Protección de Identidad (ver Sección 4.5).

- RESERVADO (1 octeto): No utilizado, debe contener ceros.

- Longitud de la Carga (2 octetos): Longitud en octetos de toda la carga SA, incluyendo la carga SA, todas las cargas de la Propuesta y todas las cargas de Trasformación asociadas con la SA propuesta.

- Dominio de Interpretación (4 octetos): Identifica el DOI (como se describe en la Sección 2.1) bajo el cual la negociación se esta llevando a cabo. El DOI es un número entero sin signo de 32 bits. Un valor de DOI de cero durante el intercambio de la Fase 1 específica una SA ISAKMP genérica la cual puede ser usada por cualquier protocolo durante el intercambio de la Fase 2. Los Atributos SA necesarios están definidos en A.4. Un valor de DOI de 1 es asignado al DOI IPsec [IPDOI]. Todos los otros valores de DOI están reservados por la IANA para usos futuros. La IANA normalmente no asignará un valor a un DOI sin referirse a alguna especificación futura, tal como un futuro RFC. Otros DOI pueden ser definidos usando la descripción del Apéndice B. Este campo DEBE estar presente en la carga SA.

- Situación (longitud variable): Un campo específico del DOI que identifica la situación bajo la cual la negociación se esta llevando a cabo. La Situación es usada para tomar las decisiones

de política concerniente a los atributos de seguridad que están siendo negociadas. Las especificaciones para la Situación del DOI de Seguridad IP de la IETF se define en [IPDOI]. Este campo DEBE estar presente en la carga SA.

3.5 Carga de la Propuesta

La Carga de la Propuesta contiene información usada durante la negociación de la SA. La propuesta consiste en mecanismos de seguridad, o trasformaciones, que serán usados para asegurar el canal de comunicaciones. La Figura 6 muestra el formato de la Carga de la Propuesta. Una descripción de su uso puede encontrarse en la Sección 4.2.

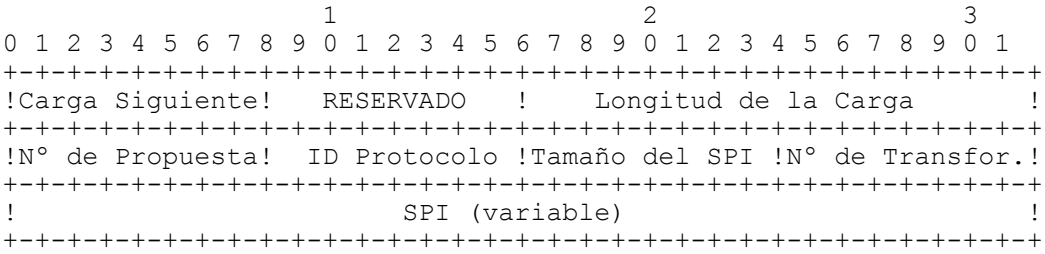


Figura 6: Formato de la Carga de la Propuesta

Los campos de la Carga de la Propuesta se definen de la siguiente forma:

- Carga siguiente (1 octeto): Identificador del tipo de carga de la siguiente carga en el mensaje. Este campo DEBE contener solamente el valor 2 o cero. Si hay Cargas de la Propuesta adicionales en el mensaje, este campo tendrá el valor 2. Si la carga de la Propuesta actual es la última dentro de la propuesta de la SA, este campo tendrá el valor cero.

- RESERVADO (1 octeto): No utilizado, debe contener ceros.

- Longitud de la Carga (2 octetos): Longitud en octetos de toda la carga de la Propuesta, incluyendo la cabecera de carga genérica, la carga de la Propuesta, y todas las cargas de Transformación asociadas con esta propuesta. En el caso de que existan múltiples propuestas con el mismo número de propuesta (ver la Sección 4.2), el campo Longitud de la Carga solamente se aplica a la carga de la Propuesta actual y no a todas.

- Número de Propuesta (1 octeto): Identificador del número de Propuesta para la carga actual. Una descripción del uso de este campo se encuentra en la Sección 4.2.

- Identificador de Protocolo (1 octeto): Especifica el Identificador de Protocolo para la negociación actual. Ejemplos pueden incluir ESP IPSEC, AH IPSEC, OSPF, TLS, etc.

- Tamaño del SPI (1 octeto): La longitud en octetos del SPI como es definido por el Identificador de Protocolo. En el caso de ISAKMP, el par de cookies del Iniciador y del Respondedor de la Cabecera de ISAKMP es el SPI de ISAKMP, por lo tanto, el Tamaño del SPI es irrelevante y PUEDE variar desde 0 a 16. Si el Tamaño del SPI no es cero, el contenido del campo de SPI DEBE ser ignorado. Si el Tamaño del SPI no es múltiplo de 4 octetos tendrá algún tipo de incidencia en el campo del SPI y de la alineación de todas las cargas en el mensaje. El DOI establecerá el tamaño del SPI para otros protocolos.

- Número de Trasformaciones (1 octeto): Especifica el número de trasformaciones de la Propuesta. Cada uno de estos está contenido en una carga de Transformación.

- SPI (variable): El SPI de la entidad emisora. En el caso de que el Tamaño del SPI no sea múltiplo de 4 octetos, no habrá relleno aplicable a la carga, sin embargo, este puede ser aplicado al final del mensaje.

El tipo de carga para la Carga de la Propuesta es dos (2)

3.6 Carga de Transformación

La Carga de Transformación contiene información usada durante la negociación de la SA. La Carga de Transformación consiste en un mecanismo de seguridad específico, o trasformaciones, con el objetivo de asegurar el canal de comunicación. La carga de Transformación también contiene los atributos SA asociados con la transformación específica. Estos atributos SA están especificados en el DOI. La Figura 7 muestra el formato de la Carga de Transformación. Una descripción de su uso puede ser encontrado en la Sección 4.2.

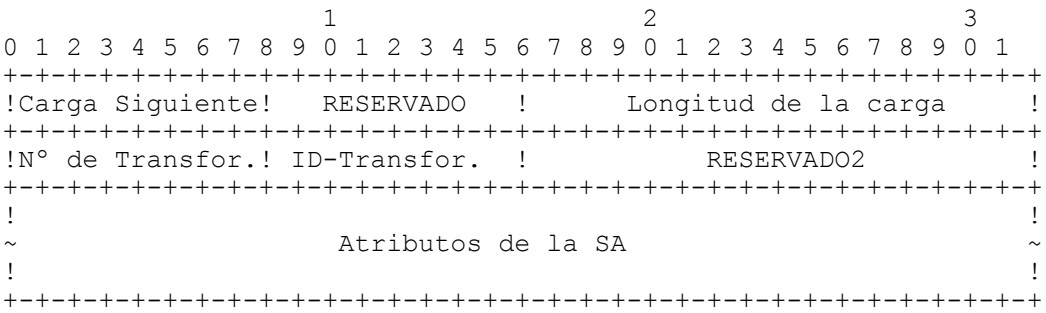


Figura 7: Formato de la Carga de Transformación

Los campos de la Carga de Transformación se definen de la siguiente forma:

- Carga siguiente (1 octeto): Identificador del tipo de carga de la siguiente carga en el mensaje. Este campo solamente DEBE contener el valor 3 o cero. Si hay cargas de Transformación adicionales en la propuesta, este campo contendrá el valor 3. Si la carga de Transformación actual es la última dentro de la propuesta, este campo contendrá el valor cero.

- RESERVADO (1 octeto): No utilizado, debe contener ceros.

- Longitud de la carga (2 octetos): La longitud en octetos de la presente carga, incluyendo la cabecera de carga genérica, valores de Transformación, y todos los Atributos SA.

- Número de transformación (1 octeto): Identifica el número de Transformación de la presente carga. Si hay más de una transformación propuesta para un protocolo específico, dentro de la carga de transformación, cada carga de Transformación tiene un único Número de Transformación. Una descripción del uso de este campo se encuentra en la Sección 4.2.

- Identificador de Transformación (1 octeto): Especifica el identificador de Transformación para el protocolo dentro de la propuesta actual. Estas trasformaciones están definidas por el DOI y dependen del protocolo que se está negociando.

- RESERVADO2 (1 octeto): No utilizado, debe contener ceros.

- Atributos SA (longitud variable): Este campo contiene los atributos de la SA como están definidos para la trasformación dada en el campo Identificador de Transformación. Los Atributos

SA se BEBERÍAN representar usando el formato de los Atributos de los Datos descriptos en la Sección 3.3. Si los atributos de la SA no están alineados en límites de 4 byte, las cargas subsiguientes no estarán alineadas y algún tipo de relleno será agregado al final del mensaje para crear un mensaje alineado a 4 octetos.

El tipo de carga para la Carga de Transformación es tres (3)

3.7 Carga de Intercambio de Claves

La Carga de Intercambio de Claves soporta una variedad de técnicas de intercambio de claves. Ejemplos de intercambio de claves son Oakley [Oakley], Diffie-Hellman, el intercambio de claves mejorado de Diffie-Hellman descripto en x9.42 [ANSI], y el intercambio de claves basado en RSA usado por PGP. La Figura 8 muestra la Carga de Intercambio de Claves.

Los campos de la Carga de Intercambio de Claves se definen de la siguiente forma:

- Carga siguiente (1 octeto): Identificador del tipo de carga de la siguiente carga en el mensaje. Si la carga actual es la última en el mensaje, este campo contendrá el valor cero.

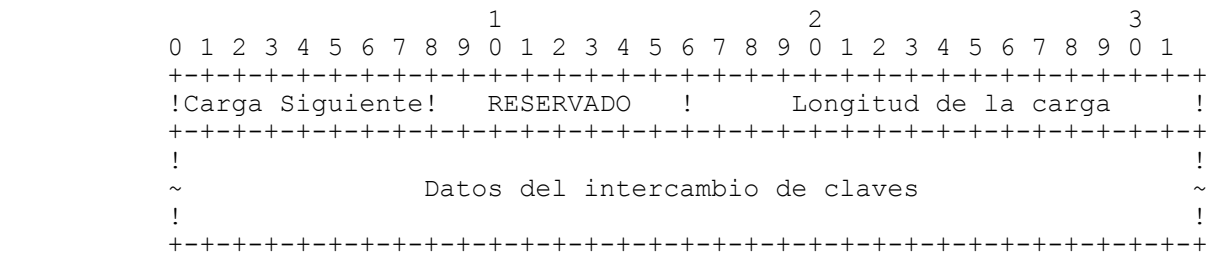


Figura 8: Formato de la Carga de Intercambio de Claves

- RESERVADO (1 octeto): No utilizado, debe contener ceros.

- Longitud de la Carga (2 octetos): Longitud en octetos de la carga actual, incluyendo la cabecera de carga genérica.

- Datos del Intercambio de Claves (longitud variable): Datos requeridos para generar una clave de sesión. La interpretación de este dato es especificado por el DOI y por el algoritmo de Intercambio de Claves asociado. Este campo también puede contener indicadores de claves pre-ubicadas [pre-placed].

El tipo de carga para la Carga de Intercambio de Claves es cuatro (4)

3.8 Carga de Identificación

La Carga de Identificación contiene datos específicos del DOI usados para intercambiar información de identificación. Esta información es usada para determinar las identidades de los usuarios de la comunicación y puede ser usada para determinar la autentificación de la información. La Figura 9 muestra el formato de la Carga de Identificación.

Los campos de la Carga de identificación se definen de la siguiente forma:

- Carga Siguiente (1 octeto): Identificador del tipo de carga de la siguiente carga en el mensaje. Si la carga actual es la última en el mensaje, este campo contendrá el valor cero.

- RESERVADO (1 octeto): No utilizado, debe contener ceros.

- Longitud de la Carga (2 octetos): La longitud en octetos de la carga actual, incluyendo la cabecera de carga genérica.

- Tipo de Identificador (1 octeto): especifica el tipo de Identificación que se está usando.

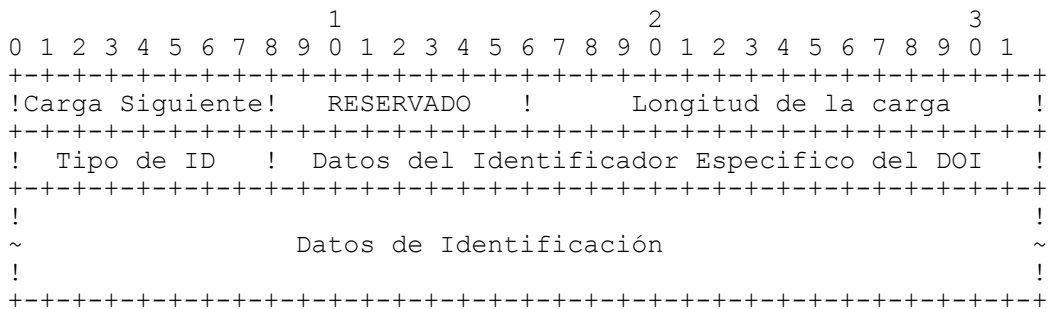


Figura 9: Formato de la Carga de Identificación

Este campo es dependiente del DOI

- Datos del Identificador Especifico del DOI (3 octetos): Contiene los datos de Identificación específicos del DOI. Si este campo no es usado, DEBE contener ceros.

- Datos de Identificación (Longitud variable): contiene información de identidad. Los valores para este campo son específicos del DOI y el formato es especificado por el campo Tipo de Identificador.

Los detalles específicos para los Datos de Identificación del DOI de Seguridad IP de la IETF se detallan en [IPDOI].

El tipo de carga para la Carga de Identificación es cinco (5).

3.9 Carga de Certificado

La Carga de Certificado proporciona un medio para trasportar certificados o otra certificación relacionada con la información vía ISAKMP y puede aparecer en cualquier mensaje ISAKMP. Las cargas de Certificado DEBERÍAN estar incluidas en un intercambio siempre que un apropiado servicio de directorio (por ejemplo DNS seguros [DNSSEC]) no esté disponible para distribuir los certificados. La Carga de Certificado DEBE ser aceptada en cualquier momento durante el intercambio. La Figura 10 muestra el formato de la Carga de Certificado.

NOTA: Los tipos de Certificados y formatos, generalmente no están ligados a un DOI. Se espera que existan solamente pocos tipos de certificaciones, y que la mayoría de los DOIs acepten estos tipos.

Los campos de la Carga de Certificado están definidos de la siguiente manera:

- Carga Siguiente (1 octeto): Identificador del tipo de carga de la siguiente carga en el mensaje. Si la carga actual es la última en el mensaje, este campo contendrá el valor cero.

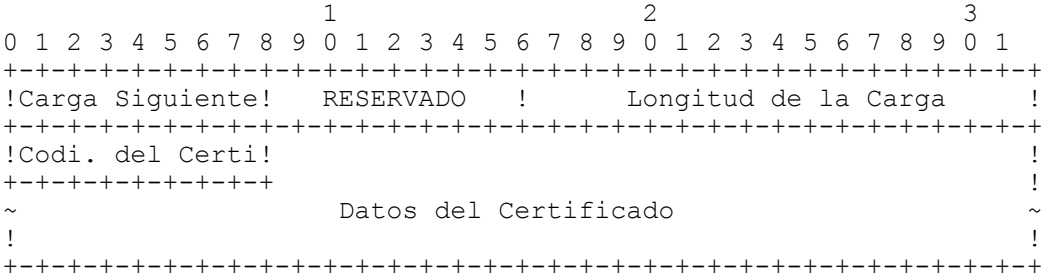


Figura 10: Formato de la Carga de Certificado.

- RESERVADO (1 octeto): No utilizado, debe contener ceros.

- Longitud de la Carga (2 octetos): Longitud en octetos de la carga actual, incluyendo la cabecera de carga genérica.

- Codificación del Certificado (1 octeto): Este campo indica el tipo de certificado o certificados relacionados a la información contenida en el campo de Datos del Certificado.

Tipos de Certificado	Valor
Ninguno	0
PKCS N°7 encapsulado en certificados X.509	1
Certificados PGP	2
Clave designada por DNS	3
Certificados X.509-firma	4
Certificados X.509-intercambio de claves	5
Tokens Kerberos	6
Lista de Revocación de Certificados (CRL)	7
Lista de Revocación de Autoridad (ARL)	8
Certificados SPKI	9
Certificados X.509- Atributos	10
RESERVADO	11-255

- Datos del certificado (longitud variable): Codificación actual de los datos del certificado. El tipo de certificación está indicado por el campo Codificación del Certificado.

El tipo de carga para la Carga de Certificado es seis (6).

3.10 Carga de Solicitud de Certificado

La Carga de solicitud de Certificado proporciona un medio para solicitar certificados vía ISAKMP y puede aparecer en cualquier mensaje. Las cargas de solicitud de Certificado DEBERÍAN estar incluidas en un intercambio siempre que un apropiado servicio de directorio (por ejemplo DNS seguros [DNSSEC]) no este disponible para distribuir los certificados. La carga de Solicitud de Certificado DEBE ser aceptada durante cualquier momento del intercambio. El respondedor de la carga de Solicitud de Certificado DEBE enviar su certificado, en el caso de que los certificados sean soportados, basados en los valores contenidos en la carga. Si múltiples certificados son requeridos, múltiples cargas de Solicitud de Certificados DEBERÍAN ser enviadas. La Figura 11 muestra el formato de la Carga de Solicitud de Certificado.

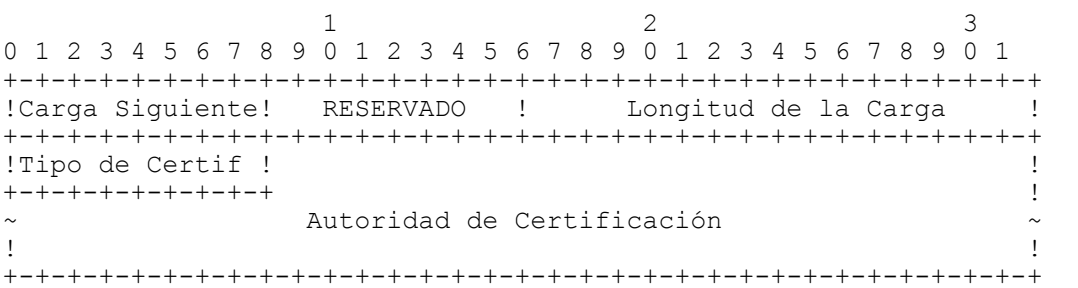


Figura 11: Formato de la Carga de solicitud de Certificado

Los campos de carga de Solicitud de Certificado son los siguientes:

- Carga Siguiente (1 octeto): Identificador del tipo de carga de la siguiente carga en el mensaje. Si la carga actual es la última en el mensaje, este campo contendrá el valor cero.

- RESERVADO (1 octeto): No utilizado, debe contener ceros.

- Longitud de la Carga (2 octetos): la longitud de la carga actual en octetos, incluyendo la cabecera de carga genérica.

- Tipo de Certificado (1 octeto): contiene una codificación del tipo de certificado requerido. Valores aceptables se encuentran en la Sección 3.9.

- Autoridad de Certificación (longitud variable): Contiene una codificación de una autoridad de certificados aceptables para el tipo de certificado solicitado. Como un ejemplo, para un certificado X.509 este campo contendrá la codificación del Nombre Distintivo del Nombre de la Entidad Emisora de una autoridad de certificación X.509 aceptable por el emisor de esta carga. Esta sería incluida para asistir al respondedor en la determinación de cuánto de esa cadena de certificación necesitaría ser enviada en respuesta a esta solicitud. Si no hay una autoridad de certificación específica requerida, este campo no DEBERÍA ser incluido.

El tipo de carga para la Carga de solicitud de Certificado es siete (7).

3.11 Carga Hash

La Carga Hash contiene los datos generados por la función hash (seleccionada durante el intercambio del establecimiento de la SA), sobre una cierta parte del mensaje y/o del estado de ISAKMP. Esta

carga puede ser usada para verificar la integridad de los datos en un mensaje ISAKMP, o para la autentificación de las entidades de la negociación. La Figura 12 muestra el formato de la Carga Hash.

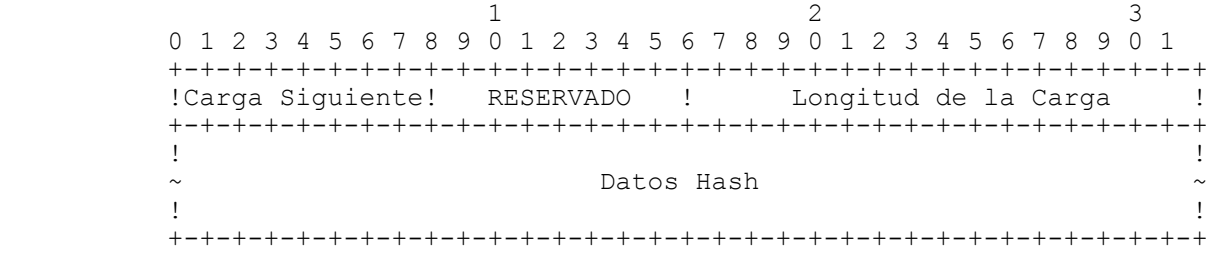


Figura 12: Formato de la carga Hash.

Los campos de la Carga de Hash se definen de la siguiente manera:

- Carga Siguiente (1 octeto): Identificador del tipo de carga de la siguiente carga en el mensaje. Si la carga actual es la última en el mensaje, este campo contendrá el valor cero.

- RESERVADO (1 octeto): No utilizado, debe contener ceros.

- Longitud de la Carga (2 octetos): la longitud de la carga actual en octetos, incluyendo la cabecera de carga genérica.

- Datos Hash (longitud variable): Datos que resultad de aplicar la rutina de hash para el mensaje ISAKMP y/o su estado.

El tipo de carga para la Carga Hash es ocho (8).

3.12 Carga de la Firma

La Carga de la Firma contiene generalmente datos para la función de la firma digital (seleccionadas durante el intercambio del establecimiento de la SA), sobre cierta parte del mensaje y/o del estado de ISAKMP. Esta carga es usada para verificar la integridad de los datos en un mensaje ISAKMP y puede ser usada para servicios de no repudio. La Figura 13 muestra el formato de la Carga de la Firma.

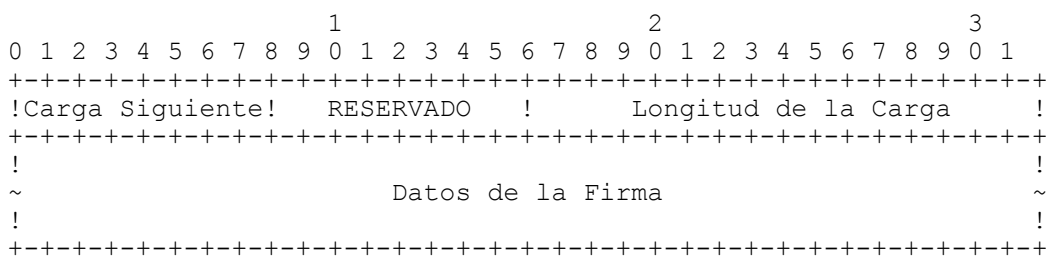


Figura 13: Formato de la Carga de la Firma

Los campos de la Carga de la Firma se definen de la siguiente manera:

- Carga Siguiente (1 octeto): Identificador del tipo de carga de la siguiente carga en el mensaje. Si la carga actual es la última en el mensaje, este campo contendrá el valor cero.

- RESERVADO (1 octeto): No utilizado, debe contener ceros.

- Longitud de la Carga (2 octetos): Longitud de la carga actual en octetos, incluyendo la cabecera de carga genérica.

- Datos de la Firma (longitud variable): Los datos que resultan de aplicar la función de una firma digital al mensaje y/o estado de ISAKMP.

El tipo de carga para la Carga de la Firma es nueve (9).

3.13 Carga Nonce

La Carga Nonce contiene información aleatoria para garantizar la vida de la conexión durante un intercambio y para proteger contra ataques de reenvío. La Figura 14 muestra el formato de la Carga Nonce. Si el nonce es usado para un intercambio de clave particular, el uso de la carga nonce será dictaminado por el intercambio de claves. El nonce puede ser trasmitido como parte de los datos del intercambio de claves, o como una carga separada. Sin embargo, esta es definida por el intercambio de claves, y no por ISAKMP.

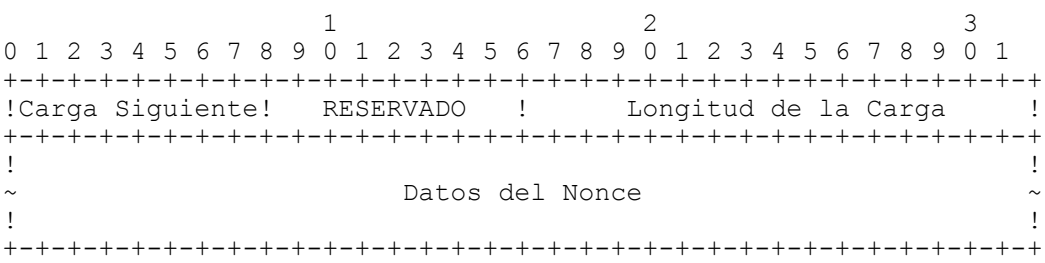


Figura 14: Formato de la Carga Nonce

Los campos de la Carga Nonce son definidos de la siguiente manera:

- Carga Siguiente (1 octeto): Identificador del tipo de carga de la siguiente carga en el mensaje. Si la carga actual es la última en el mensaje, este campo contendrá el valor cero.

- RESERVADO (1 octeto): No utilizado, debe contener ceros.

- Longitud de la Carga (2 octetos): Longitud de la carga actual en octetos, incluyendo la cabecera de carga genérica.

- Datos del Nonce (longitud variable): contiene información aleatoria generada por la entidad transmisora.

El tipo de carga para la Carga Nonce es diez (10).

3.14 Carga de Notificación

La Carga de Notificación puede incluir datos ISAKMP y datos específicos del DOI y se utiliza para trasmitir datos informativos, tales como condiciones de error, en entidades pares de ISAKMP. Es posible enviar múltiples cargas de Notificación en un único mensaje ISAKMP. La Figura 15 muestra el formato de la Carga de Notificación.

La notificación que ocurre durante, o que se refiere a, la negociación de la Fase 1 es identificada por el par de cookies del Iniciador y del Respondedor en la Cabecera de ISAKMP. El Identificador de Protocolo, en este caso, es ISAKMP y el valor del SPI es cero porque el par de cookies en la Cabecera ISAKMP identifican a la SA ISAKMP. Si la notificación ocurre antes de que se haya completado el intercambio de información de las claves, entonces la Notificación estará desprotegida.

La notificación que ocurre durante, o se refiere a, la Fase 2 de la negociación es identificada por el par de cookies del Iniciador y del Respondedor en la Cabecera de ISAKMP y el Identificador de Mensajes y

el SPI asociados con la negociación actual. Un ejemplo de este tipo de notificación es usado para indicar por qué una propuesta fue rechazada.

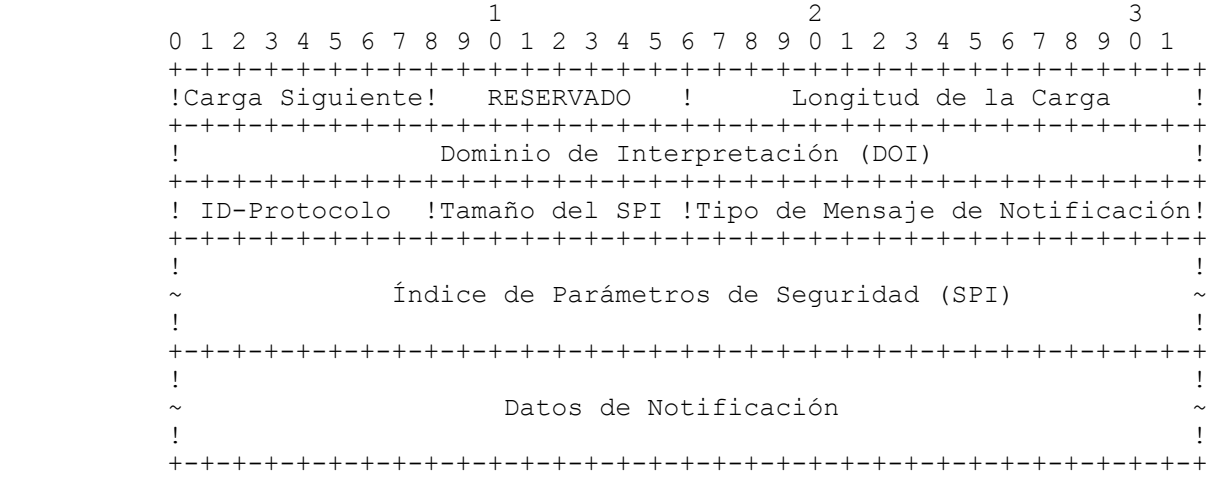


Figura 15: Formato de la Carga de Notificación

Los campos de la Carga de Notificación se definen de la siguiente manera:

- Carga Siguiente (1 octeto): Identificador del tipo de carga de la siguiente carga en el mensaje. Si la carga actual es la última en el mensaje, este campo contendrá el valor cero.

- RESERVADO (1 octeto): No utilizado, debe contener ceros.

- Longitud de la Carga (2 octetos): Longitud de la carga actual en octetos, incluyendo la cabecera de carga genérica.

- Dominio de Interpretación (4 octetos): Identifica el DOI (como está descripto en la Sección 2.1) bajo el cual esta notificación esta tomando lugar. Para ISAKMP este valor es cero (0) y para el DOI IPsec es uno (1). Otros DOIs pueden ser definidos usando la descripción del Apéndice B.

- Identificador de Protocolo (1 octeto): Especifica el identificador del protocolo para la notificación actual. Ejemplo pueden incluir ISAKMP, ESP IPsec, AH IPsec, OSPF, TLS, etc.

- Tamaño del SPI (1 octeto): La longitud en octetos del SPI como es definido por el Identificador de Protocolo. En el caso de ISAKMP, el par de cookies del Iniciador y del Respondedor de la Cabecera ISAKMP es el SPI de ISAKMP, por lo tanto, el Tamaño del SPI es irrelevante y PUEDE variar desde cero (0) a dieciséis (16). Si el Tamaño del SPI no es cero, el contenido del campo del SPI DEBE ser ignorado. El Dominio de Interpretación (DOI) determinará el tamaño del SPI para otros protocolos.

- Tipo de Mensaje de Notificación (2 octetos): Especifica el tipo de mensaje de notificación (ver Sección 3.14.1). Textos adicionales, si es especificado por el DOI, son colocados en el campo de Datos de Notificación.

- SPI (longitud variable): Índice de Parámetros de Seguridad. El SPI de la entidad receptora. El uso del campo SPI se describió en la Sección 2.4. La longitud de este campo es determinada por el campo de Tamaño del SPI y no necesariamente se debe alinear a límites de 4 octetos.

- Datos de Notificación (longitud variable): Datos informativos o de error trasmitidos además del Tipo de Mensaje de Notificación. Los valores para este campo son específicos del DOI

El tipo de carga para la Carga de Notificación es once (11).

3.14.1 Tipos de Mensaje de Notificación

La información de notificación puede tener mensajes de error especificando por qué una SA no pudo ser establecida. También puede tener datos de estado para que un manejador de procesos en una base de datos de SA pueda comunicarse con los procesos pares. Por ejemplo, una interfaz de usuario segura [secure front end] o un security gateway pueden usar el Mensaje de Notificación para sincronizar la comunicación de SA. La tabla siguiente enumera los tipos de Mensajes de Notificación y sus valores correspondientes. Los valores en el rango de Uso Privado se espera que sean valores específicos del DOI.

MENSAJES DE NOTIFICACIÓN - TIPOS DE ERRORES

Errores	Valor
TIPO DE CARGA NO VÁLIDA	1
DOI NO SOPORTADO	2
SITUACIÓN NO SOPORTADA	3
COOKIE NO VÁLIDO	4
VERSIÓN MAYOR NO VÁLIDA	5
VERSIÓN MENOR NO VÁLIDA	6
TIPO DE INTERCAMBIO NO BALIDO	7
BANDERAS NO VALIDAS	8
IDENTIFICADOR DE MENSAJE NO VÁLIDO	9
IDENTIFICADOR DE PROTOCOLO NO VÁLIDO	10
SPI NO VÁLIDO	11
IDENTIFICADOR DE TRANSFORMACIÓN NO VÁLIDO	12
ATRIBUTOS NO SOPORTADOS	13
ELECCIÓN DE LA PROPUESTA NO VÁLIDA	14
SINTAXIS DE LA PROPUESTA DEFICIENTE	15
CARGA MAL FORMADA	16
INFORMACIÓN DE CLAVE NO VÁLIDA	17
INFORMACIÓN DEL IDENTIFICADOR NO VÁLIDO	18
CODIFICACIÓN DE CERTIFICADO NO VÁLIDO	19
CERTIFICADO NO VÁLIDO	20
TIPO DE CERTIFICADO NO SOPORTADO	21
AUTORIDAD DE CERTIFICACIÓN NO VÁLIDA	22
INFORMACIÓN DE HASH NO VÁLIDA	23
ERROR EN LA AUTENTIFICACIÓN	24
FIRMA NO VÁLIDA	25
NOTIFICACIÓN DE DIRECCIÓN	26
NOTIFICACIÓN DE TIEMPO DE VIDA DE LA SA	27
CERTIFICADO NO DISPONIBLE	28
TIPO DE INTERCAMBIO NO SOPORTADO	29
RESERVAD (Uso Futuro)	31-8191
USO PRIVADO	8192-16383

MENSAJE DE NOTIFICACIÓN - TIPOS DE STATUS

Estado	Valor
CONECTADO	16384
RESERVADO (Uso Futuro)	16385 - 24575
Códigos específicos de DOI	24576 - 32767
USO PRIVADO	32768 - 40959
RESERVADO (Uso futuro)	40960 - 65535

3.15 Carga de Cancelación

La Carga de Cancelación contiene un identificador de SA específico de un protocolo que el emisor ha revocado para esta base de datos de SA y por consiguiente ya no es válida. La Figura 16 muestra el formato de la Carga de Cancelación. Es posible enviar múltiples SPIs en una carga de Cancelación, sin embargo, cada SPI DEBE ser del mismo protocolo. La mezcla de identificadores de protocolo NO DEBE ser realizada en la carga de Cancelación.

La cancelación concerniente a una SA ISAKMP contendrá un Identificador de Protocolo de ISAKMP y los SPIs son las cookies del Iniciador y Respondedor de la Cabecera de ISAKMP. La cancelación concerniente a una SA de Protocolo, tales como ESP o AH, contendrán el Identificador de Protocolo de ese protocolo (por ejemplo ESP, AH) y la SPI son las SPIs de la entidades emisoras.

Nota: La Carga de Cancelación no es una solicitud del respondedor para cancelar una SA, sino que es una notificación del iniciador al respondedor. Si el respondedor elige ignorar el mensaje, la siguiente comunicación del respondedor al iniciador, que use esa SA, fallará. Se espera que un respondedor reconozca el acuse de recibo de la carga de Cancelación.

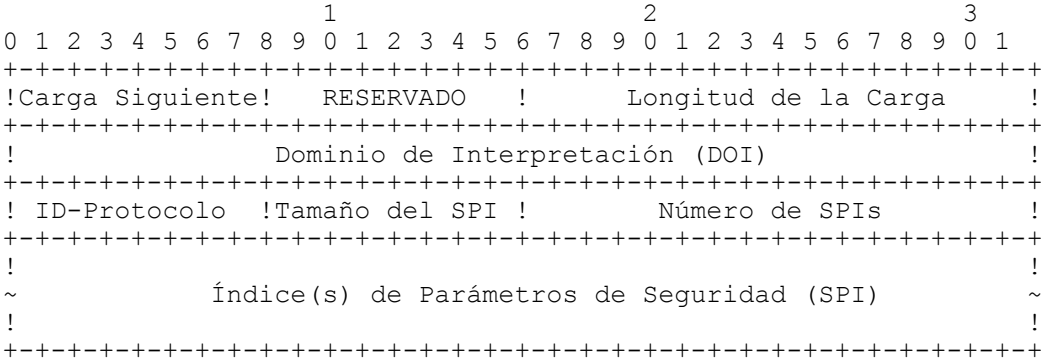


Figura 16: Formato de la Carga de Cancelación

Los campos de la Carga de Cancelación se definen de la siguiente manera:

- Carga Siguiente (1 octeto): Identificador del tipo de carga de la siguiente carga en el mensaje. Si la carga actual es la última en el mensaje, este campo contendrá el valor cero.

- RESERVADO (1 octeto): No utilizado, debe contener ceros.

- Longitud de la Carga (2 octetos): Longitud de la carga actual en octetos, incluyendo la cabecera de carga genérica.

- Dominio de Interpretación (4 octetos): Identifica el DOI (como se describe en la Sección 2.1) bajo el cual esta cancelación esta tomando lugar. Para ISAKMP este valor es cero (0) y para el DOI IPsec es uno (1). Otros DOIs pueden ser definidos usando la descripción del Apéndice B

- Identificador de Protocolo (1 octeto): ISAKMP puede establecer SA para varios protocolos, incluyendo ISAKMP y IPsec. Este campo identifica a qué base de datos de asociaciones de seguridad (SAD) se aplicará la solicitud de cancelación.

- Tamaño del SPI (1 octeto): Longitud en octetos del SPI como esta definido por el Identificador de Protocolo. En el caso de ISAKMP, el par de cookies del Iniciador y del Respondedor es el SPI de ISAKMP. En este caso el Tamaño del SPI sería de 16 octetos para cada uno de los SPI que están siendo cancelados.

- Número de SPIs (2 octetos): El número de SPIs contenidos en la Carga de Cancelación. El tamaño de cada SPI es definido por el campo Tamaño del SPI.

- Índice(s) de parámetros de seguridad (longitud variable): identifica la SA(s) que serán canceladas. Los valores para este campo están en el DOI y protocolo especifico. La longitud de este campo es determinada por los campos Tamaño del SPI y Número de SPIs.

El tipo de carga para la carga de Cancelación es doce (12)

3.16 Carga de Identificador del Vendedor

La Carga de Identificador del Vendedor contiene una constante definida por el vendedor. La constante es usada por los vendedores para identificar y reconocer instancias remotas de sus aplicaciones. Este mecanismo permite a un vendedor experimentar nuevas características, manteniendo la compatibilidad. Esto no es una habilidad de ISAKMP. La Figura 17 muestra la Carga de Identificación de Vendedor.

La carga de Identificación del Vendedor no es un anuncio de que el emisor enviará tipos de cargas privadas. Un vendedor que envía un Identificador de vendedor no DEBE hacer ninguna conjetura sobre cargas privadas que podrían ser enviadas a menos que un Identificador de Vendedor sea también recibido. Múltiples cargas de Identificador

de Vendedor PUEDEN ser enviadas. Una implementación NO REQUIERE comprender las cargas de Identificación de Vendedor. Una implementación NO REQUIERE enviar todas las cargas de Identificación de Vendedor. Si una carga privada fue enviada, sin acuerdo previo, una implementación puede rechazar una propuesta con un mensaje de notificación TIPO DE CARGA NO VÁLIDA.

Si una Carga de Identificador de Vendedor es enviada, esta DEBE ser enviada durante la primera fase de la negociación. La recepción de una carga de Identificador de Vendedor familiar en la fase uno de la negociación permite que una implementación haga uso de los números de carga de Uso Privado (128 a 255), descriptos en la Sección 3.1 para extensiones especificas del vendedor durante la fase dos de la negociación. La definición de "familiar" se usa para determinar implementaciones. Algunos vendedores pueden desear implementar otras extensiones de vendedor antes de la estandarización. No obstante, esta práctica no DEBERÍA difundirse y los vendedores deben trabajar hacia una estandarización.

La constante definida por el vendedor DEBE ser única. La elección del hash y el texto a hashiar la decide el vendedor. Como ejemplo, los vendedores pueden generar su identificador de vendedor tomando un simple hash de la cadena de caracteres que contiene el nombre del producto, y la versión del producto.

Un hash es usado en lugar de un registro de vendedor para evitar problemas de políticas criptográficas locales con listas de productos "aprobados", para evitar tener una lista de vendedores, y permitiendo evitar que productos clasificados aparezcan en alguna lista. Por ejemplo:

"Compañía IPsec. Versión 97.1"

(no incluido textualmente) Tiene un hash MD5 igual a: 48544f9b1fe662af98b9b39e50c01a5a, cuando se usa MD5FILE. Los vendedores pueden incluir todo el hash, o solo una parte, como parte de los datos de la carga. Hay implementaciones de seguridad de este hash por lo tanto su elección es arbitraria.

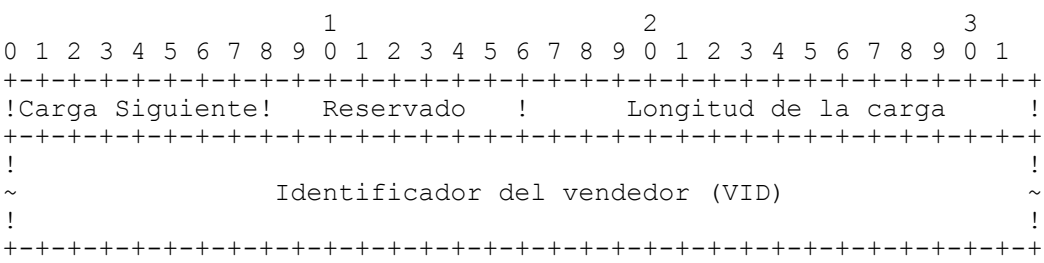


Figura 17: Formato de la Carga de Identificador del Vendedor

La Carga de Identificación del Vendedor esta definida de la siguiente manera:

- Carga Siguiente (1 octeto): Identificador del tipo de carga de la siguiente carga en el mensaje. Si la carga actual es la última en el mensaje, este campo contendrá el valor cero.

- RESERVADO (1 octeto): No utilizado, debe contener ceros.

- Longitud de la Carga (2 octetos): Longitud de la carga actual en octetos, incluyendo la cabecera de carga genérica.

- Identificador del vendedor (longitud variable): Hash de la cadena de caracteres del vendedor más la versión (como se describió arriba).

El tipo de carga para la Carga de Identificador del Vendedor es trece (13).

4 Intercambios ISAKMP

ISAKMP proporciona la sintaxis básica para el intercambio de un mensaje. Los bloques básicos de construcción para los mensajes ISAKMP son los tipos de carga descriptos en la Sección 3. Esta sección describe los procedimientos para el establecimiento y modificación de SAs, seguidos de un conjunto de intercambios por defecto que PUEDEN ser usados para una interoperatibilidad inicial. Otros intercambios serán definidos teniendo en cuenta el DOI y el intercambio de claves. El [IPDOI] y el [IKE] son ejemplos de cómo esto es logrado. El Apéndice B explica los procedimientos para lograr estas inclusiones.

4.1 Tipos de Intercambios ISAKMP

ISAKMP permite la creación de intercambios para el establecimiento de SA y material claves. Hay actualmente 5 Tipos de Intercambio por

defecto definidos por ISAKMP. Desde la Sección 4.4 hasta la Sección 4.8 se describen estos intercambios. Los intercambios definen los contenidos y el ordenamiento de los mensajes ISAKMP entre usuarios. La mayoría de los intercambios incluirán todos los tipos de cargas básicas - SA, KE, ID, SIG, y pueden incluir otros. La diferencia principal entre los tipos de intercambio es el ordenamiento de los mensajes y el ordenamiento de las cargas dentro de cada mensaje. Mientras que el ordenamiento de las cargas dentro de los mensajes no esta definido, para el procesamiento eficiente se RECOMIENDA que la carga de SA sea la primer carga dentro de un intercambio. El procesamiento de cada carga dentro de un intercambio se describe en la Sección 5.

Desde la Sección 4.4 hasta la Sección 4.8 se ofrece un conjunto de intercambios ISAKMP por defecto. Estos intercambios proporcionan diferentes protecciones de seguridad para el intercambio mismo y la información intercambiada. Los diagramas en cada una de las siguientes secciones muestran el ordenamiento del mensaje para cada tipo de intercambio, como así también las cargas incluidas en cada mensaje, y proporcionan notas básicas que describen que ha sucedido después de cada mensaje intercambiado. Ninguno de estos ejemplos incluyen "cargas opcionales", como por ejemplo certificados o solicitud de certificado. Además, ninguno de estos ejemplos incluye un intercambio inicial de las cabeceras de ISAKMP (conteniendo las cookies del iniciador y del respondedor) que proporcionarían protección contra saturación (ver Sección 2.5.3).

Los intercambios definidos no pretenden satisfacer todos los requerimientos del DOI y de los protocolos de intercambio de claves. Si los intercambios definidos satisfacen los requerimientos del DOI, podrían ser usados como se explicó. Si los intercambios definidos no satisfacen los requerimientos de seguridad definidos por el DOI, el DOI DEBE especificar nuevos tipos de intercambio y las secuencias válidas de las cargas que hacen un intercambio exitoso, y como construir y interpretar estas cargas. Todas las implementaciones de ISAKMP DEBEN implementar Intercambios Informativos y DEBERÍAN implementar los otros 4 intercambios. Sin embargo, esto depende de la definición del DOI y de los protocolos de intercambio asociados.

Como se explicó arriba, estos tipos de intercambio pueden ser usados en cualquier fase de la negociación, no obstante, deben proporcionar diferentes propiedades de seguridad en cada una de las fases. Con cada uno de estos intercambios, la combinación de las cookies y de los campos del SPI identifican si este intercambio esta siendo usado en la primera o en la segunda fase de la negociación.

4.1.1 Notación

La siguiente notación se usa para describir los tipos de intercambio ISAKMP, como se muestra en la siguiente sección, con los formatos de los mensajes y las cargas asociadas:

HDR: Es una cabecera de ISAKMP cuyo tipo de intercambio define el ordenamiento de la carga.
SA: Es una carga de negociación SA con una o más Propuestas y cargas de Transformación. Un iniciador PUEDE proporcionar múltiples propuestas para la negociación, un respondedor DEBE contestar solo una.
KE: Es la carga de intercambio de claves.
IDx: Es la carga de identidad para "x". x puede ser "ii" o "ir" para el iniciador y respondedor de ISAKMP, respectivamente, o x puede ser "ui", "ur" (cuando un demonio de ISAKMP es un negociador proxy), para el usuario iniciador y respondedor respectivamente.
HASH: Es la carga hash.
SIG: Es la carga de la firma. Los datos a firmar son específicos del intercambio.
AUTH: Es un mecanismo de autentificación genérico, tal como HASH o SIG.
NONCE: Es la carga NONCE.
=>: Comunicación desde el "iniciador al respondedor".
<=: Comunicación desde el "respondedor al iniciador".

4.2 Establecimiento de Asociaciones de Seguridad

Las cargas, SA, la de la Propuesta, y la de Transformación son utilizadas para construir los mensajes ISAKMP para la negociación y el establecimiento de SAs. Un mensaje de establecimiento SA consiste en una única carga SA seguida de al menos una, y posiblemente muchas, cargas de Propuesta y al menos una y posiblemente muchas, cargas de Transformación asociadas con cada carga de Propuesta. Debido a que estas cargas se consideran en conjunto, las cargas SA apuntarán a cualquiera de las cargas siguientes y no a la carga de la Propuesta incluida en la carga SA. La carga SA contiene, el DOI y la situación para la SA propuesta. Cada carga de la Propuesta contiene un SPI y asegura que el SPI esta asociado con el Identificador de Protocolo en concordancia con la Arquitectura de Seguridad de Internet [SEC-ARCH]. Las cargas de la Propuestas pueden o no tener el mismo SPI, ya que es una implementación dependiente. Cada carga de Transformación contiene mecanismos de seguridad específicos para ser usados por el protocolo designado. Se espera que la Propuesta y las cargas de Transformación sean usadas solamente durante la negociación del establecimiento de la SA. La creación de cargas para la negociación y establecimiento de SA descriptas en esta sección se aplican a todos los intercambios

ISAKMP que se describen desde la Sección 4.4 hasta la Sección 4.8. Los ejemplos mostrados en el punto 4.2.1 contienen solamente las cargas, SA, la de la Propuesta, y la de Transformación, y no contienen otras cargas que podrían existir en un intercambio ISAKMP determinado.

La carga de la Propuesta proporciona a la entidad iniciadora la capacidad de presentar a la entidad que responde los protocolos de seguridad y mecanismos de seguridad asociados para el uso de la SA que esta siendo negociada. Si la negociación del establecimiento de una SA es para un conjunto combinado de protección que consiste de múltiples protocolos, DEBERÁ existir múltiples cargas de Propuesta, cada una con el mismo número de Propuesta. Estas propuestas DEBEN considerarse como una unidad y NO DEBEN estar separadas por una propuesta con un número de propuesta diferente. El uso del mismo número de Propuesta en múltiples cargas de Propuesta proporciona lógica de operación AND, es decir Protocolo 1 AND Protocolo 2. El primer ejemplo de abajo muestra un conjunto de protección ESP AND AH. Si la negociación del establecimiento de SA es para diferentes conjuntos de protección, DEBERÁN existir múltiples cargas de Propuesta cada una con un número de Propuesta incrementalmente único. Las diferentes propuestas DEBEN ser presentadas en el orden de preferencia del iniciador. El uso de diferentes números de Propuesta en múltiples cargas de Propuesta proporciona lógica de operación OR, es decir, Propuesta 1 OR Propuesta 2, donde cada propuesta puede tener más de un protocolo. El segundo ejemplo de abajo muestra un conjunto de protección AH AND ESP, OR solamente un conjunto de protección ESP. Observe que el campo Carga Siguiente de la carga de la Propuesta apunta a otra carga de la Propuesta (si existiera). La existencia de una carga de Propuesta implica la existencia de una o mas cargas de Transformación.

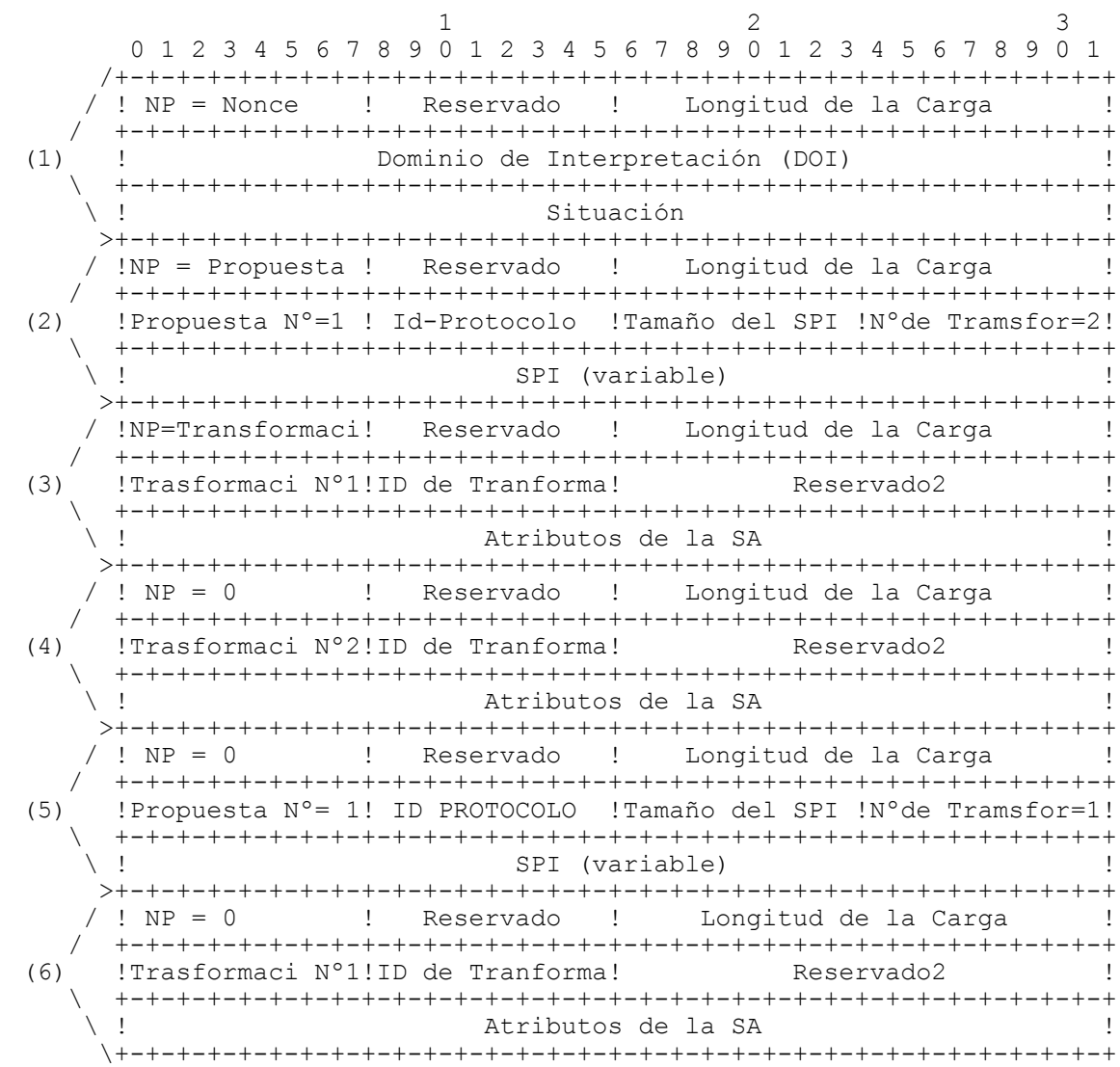
La Carga de Trasformación proporciona a la entidad iniciadora la capacidad de presentar a la entidad que responde múltiples mecanismos, o trasformaciones, para un protocolo dado. La carga de la Propuesta identifica a un Protocolo para el cual los servicios y mecanismos están siendo negociados. La carga de Transformación permite a la entidad iniciadora presentar múltiples trasformaciones posibles soportadas para el protocolo propuesto. Pueden existir muchas trasformaciones asociadas con una carga de Propuesta específica, cada una identificará una carga de Transformación separada. Las múltiples transformaciones DEBEN ser presentadas con números crecientes únicos de acuerdo al orden de preferencia del iniciador. La entidad receptora DEBE seleccionar una única transformación para cada protocolo dentro de una propuesta o rechazar la propuesta entera. El uso del número de Transformación en las cargas de Trasformaciones múltiples proporciona un segundo nivel de operación OR, es decir Trasformación 1 OR Trasformación 2 OR

Trasformación 3. El ejemplo 1 muestra 2 trasformaciones posibles para ESP y una única transformación para AH. El ejemplo 2 muestra una transformación para AH AND una transformación para ESP OR dos trasformaciones para ESP. Observe que el campo Carga Siguiente de la carga de Transformación puede apuntar hacia cero o más cargas de Transformación.

Cuando se responde a una carga SA, el respondedor DEBE enviar una carga SA con la propuesta seleccionada, la cual consistirá de múltiples cargas de Propuestas y sus cargas de Transformación asociadas. Cada una de las cargas de la Propuesta DEBE contener una única carga de Transformación asociada con el protocolo. El respondedor DEBERÍA retener el campo Número de Propuesta dentro de la carga de Propuesta y el campo Número de Transformación en cada carga de Transformación de la de la propuesta seleccionada. La retención de los números de la Propuesta y Transformación deberá acelerar el procesamiento del protocolo del iniciador por la anulación de la necesidad de comparar la selección del respondedor con cada una de las opciones ofrecidas. Estos valores permiten al iniciador realizar la comparación directa y rápidamente. El iniciador DEBE verificar que la carga SA recibida del respondedor concuerde con las propuestas enviadas inicialmente.

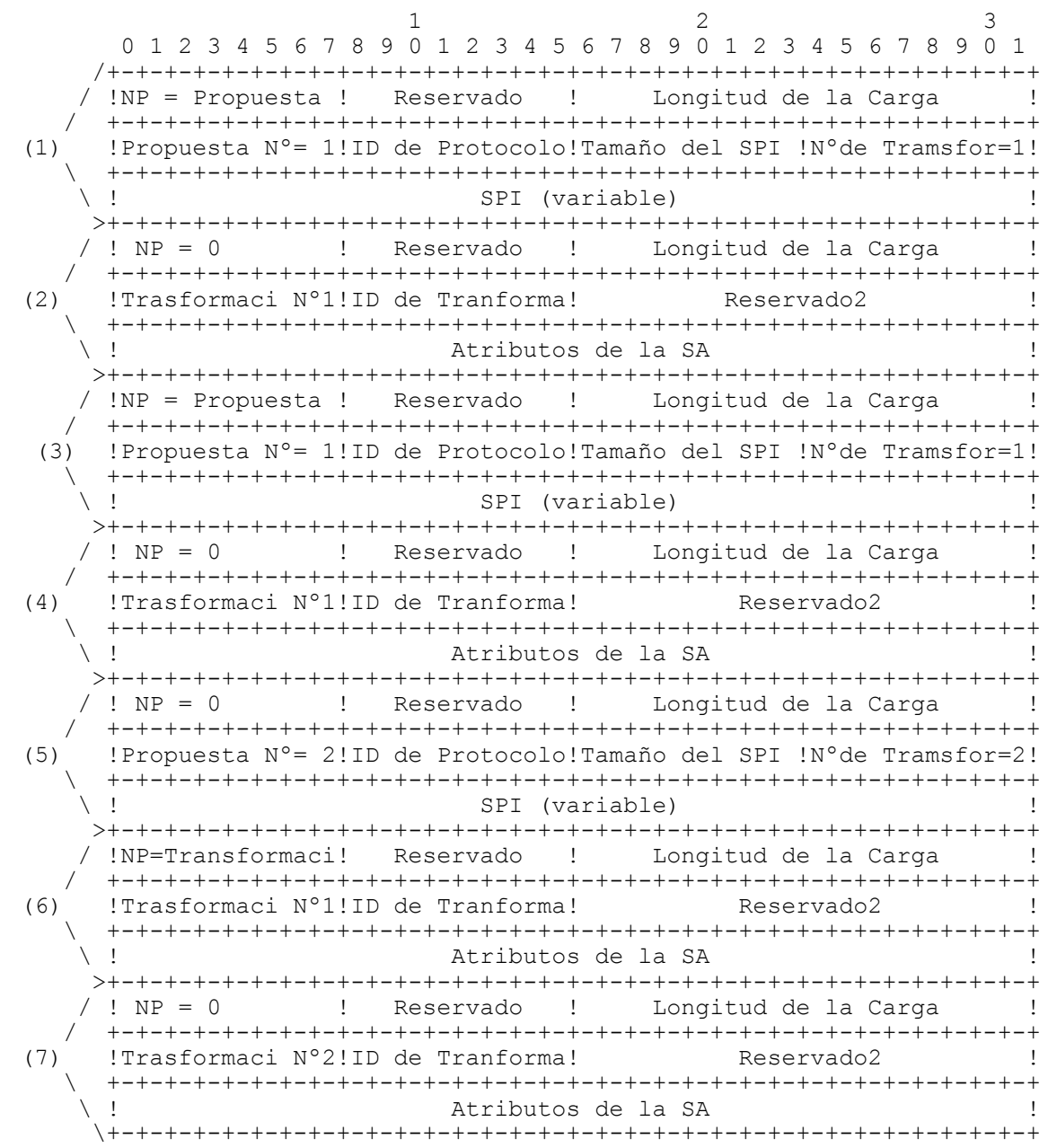
4.2.1 Ejemplos de Establecimientos de Asociaciones de Seguridad

Este ejemplo muestra una Propuesta para un conjunto de protección combinado con 2 protocolos diferentes. El primer protocolo esta presentado por dos trasformaciones soportadas por el oferente. El segundo protocolo esta presentado por una única transformación. Un ejemplo de esta propuesta puede ser: Protocolo 1 es, ESP con Transformación 1 con 3DES y Transformación 2 con DES AND Protocolo 2 es, AH con transformación 1 con SHA. El respondedor DEBE elegir de las 2 trasformaciones que propone ESP. El conjunto de protección resultante será (1) 3DES AND SHA OR (2) DES AND SHA, dependiendo de que transformación ESP fue seleccionada por el respondedor. Observe que este ejemplo es mostrado usando el Intercambio Base.
Situación



(1) = Carga SA
(2) = Propuesta 1, Protocolo 1
(3) = Transformación 1
(4) = Transformación 2
(5) = Propuesta 1, Protocolo 2
(6) = Transformación 1

Este segundo ejemplo muestra una Propuesta para 2 conjuntos de protección diferente. La carga SA fue omitida por razones de espacio. El primer conjunto de protección es presentado con una transformación para el primer protocolo y una transformación para el segundo. El segundo conjunto de protección es presentado con 2 transformaciones para un solo protocolo. Un ejemplo para esta propuesta puede ser: Propuesta 1 con Protocolo 1 con AH con Transformación 1 con MD5 AND Protocolo 2 con ESP con Transformación 1 con 3DES. Esto es seguido por la Propuesta 2 con Protocolo 1 con ESP con Transformación 1 con DES y Transformación 2 con 3DES. El respondedor DEBE seleccionar de las dos propuestas diferentes. Si la segunda Propuesta es seleccionada, el respondedor DEBE seleccionar de las dos trasformaciones para ESP. El conjunto de protección resultante será (1) MD5 AND 3DES OR la selección entre (2) DES OR (3) 3DES.


1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
!NP = Propuesta ! Reservado ! Longitud de la Carga !
(1) !Propuesta N°= 1!ID de Protocolo!Tamaño del SPI !N°de Tramsfor=1!
SPI (variable) !
! NP = 0 ! Reservado ! Longitud de la Carga !
(2) !Trasformaci N°1!ID de Tranforma! Reservado2 !
Atributos de la SA !
!NP = Propuesta ! Reservado ! Longitud de la Carga !
(3) !Propuesta N°= 1!ID de Protocolo!Tamaño del SPI !N°de Tramsfor=1!
SPI (variable) !
! NP = 0 ! Reservado ! Longitud de la Carga !
(4) !Trasformaci N°1!ID de Tranforma! Reservado2 !
Atributos de la SA !
! NP = 0 ! Reservado ! Longitud de la Carga !
(5) !Propuesta N°= 2!ID de Protocolo!Tamaño del SPI !N°de Tramsfor=2!
SPI (variable) !
!NP=Transformaci! Reservado ! Longitud de la Carga !
(6) !Trasformaci N°1!ID de Tranforma! Reservado2 !
Atributos de la SA !
! NP = 0 ! Reservado ! Longitud de la Carga !
(7) !Trasformaci N°2!ID de Tranforma! Reservado2 !
Atributos de la SA !

(1) = Propuesta 1, Protocolo 1
(2) = Transformación 1
(3) = Propuesta 1, Protocolo 2
(4) = Transformación 1
(5) = Propuesta 2, Protocolo 1
(6) = Transformación 1
(7) = Transformación 2

4.3 Modificación de SA

La modificación de una SA dentro de ISAKMP es llevada a cabo por la creación de una nueva SA y las comunicaciones que se inician usarán esa nueva SA. La cancelación de la antigua SA puede hacerse en cualquier momento después de que la nueva SA haya sido establecida. La cancelación de la antigua SA depende de la política de seguridad local. La modificación de SAs usa el método de "creación de una nueva SA seguida de la cancelación de la antigua SA" esto se hace para evitar vulnerabilidades potenciales dentro de la sincronización de la modificación de los atributos de la SA existentes. El procedimiento para la creación de nuevas SAs está definido en la Sección 4.2. El procedimiento para la cancelación de SAs esta definido en la Sección 5.15.

La modificación de una SA ISAKMP (Fase 1 de la negociación) sigue el mismo procedimiento que la creación de una SA ISAKMP. No existe relación entre las 2 SAs, y el par de cookies del iniciador y del respondedor DEBERÍAN ser diferentes, como se definió en la Sección 2.5.3.

La modificación de una SA de Protocolo (fase 2 de la negociación) sigue el mismo procedimiento que la creación de una SA de Protocolo. La creación de una nueva SA está protegida por la SA ISAKMP existente. No hay relación entre las dos SA del Protocolo. La aplicación de un protocolo no DEBERÍA comenzar a utilizar la nueva SA creada para el tráfico saliente y DEBERÍA continuar soportando el tráfico entrante en la antigua SA hasta que la SA este cancelada o hasta que el tráfico de la antigua SA este bajo la protección de la nueva SA creada. Según lo indicado anteriormente en esta sección, la cancelación de una SA antigua depende de la política de seguridad local.

4.4 Intercambio Base

El Intercambio Base esta diseñado para permitir que el Intercambio de Claves y la Autentificación relacionen información trasmitida simultáneamente. La combinación del Intercambio de Claves y la información de Autentificación relacionada dentro de un mensaje reduce el número de viajes de ida y vuelta a expensas de no

proporcionar protección de identidad. La protección de identidad no es proporcionada porque las identidades se intercambian antes de que un secreto común compartido haya sido establecido, por consiguiente, la encriptación de las identidades no es posible. El siguiente diagrama muestra los mensajes con las posibles cargas enviadas en cada mensaje y las notas de ejemplo de un Intercambio Base.

INTERCAMBIO BASE

N°	Iniciador	Dirección	Respondedor	Notas
(1)	HDR; SA; NONCE	=>		Comienzo SA-ISAKMP o negociación Proxy
(2)		<=	HDR; SA; NONCE	SA básica acordada
(3)	HDR; KE; IDii; AUTH	=>		Clave generada (por el respondedor) identidad del iniciador verificada por el respondedor
(4)		<=	HDR; KE; IDir; AUTH	Identidad del respondedor verificada por el iniciador, clave generada (por el iniciador), SA establecida

En el primer mensaje (1), el iniciador genera una propuesta que considera adecuada para proteger el tráfico en una situación dada. Las cargas, SA, la de la Propuesta, y la de Transformación son incluidas en la carga SA (con propósitos de notación). La información aleatoria usada para garantizar la vida de la conexión y protección contra ataques de reenvío también es trasmitida. La información aleatoria que proveen ambas partes DEBERÍA ser usada por el mecanismo de autentificación para proveer prueba compartida de la participación en el intercambio.

En el segundo mensaje (2), el respondedor indica el conjunto de protección que ha aceptado con la SA, la Propuesta, y la Carga de Transformación. Nuevamente, la información aleatoria que es usada para proteger contra ataques de reenvío y garantizar la vida de la conexión también es trasmitida. La información aleatoria proporcionada por ambas partes DEBERÍA ser usada por el mecanismo de autentificación para proporcionar prueba compartida de la participación en el intercambio. La política de seguridad local dictaminará la acción del respondedor si no es aceptado el conjunto de protección propuesto. Una posible acción es la transmisión de una carga de Notificación como parte de un Intercambio Informativo.

En el tercer (3) y cuarto (4) mensaje, el iniciador y el respondedor, respectivamente intercambian material clave usado para llegar a un secreto común compartido y a la identificación de la información. Esta información es trasmitida bajo la protección de una función de autentificación acordada. La política de seguridad local dictaminará la acción si un error llegara a ocurrir durante estos mensajes. Una posible acción es la transmisión de una carga de Notificación como parte de un Intercambio Informativo.

4.5 Intercambio de Protección de Identidad

El Intercambio de Protección de Identidad está diseñado para separar la información de Intercambio de Claves de la de Identidad y de la información relacionada a la Autentificación. La separación del Intercambio de Claves de la Identidad y la información relacionada a la Autentificación proporcionan protección para las entidades de la comunicación, a costa de dos mensajes adicionales. Las identidades se intercambian bajo la protección de un secreto común compartido establecido anteriormente. El siguiente diagrama muestra los mensajes con las posibles cargas enviadas en cada mensaje y las notas de ejemplo de un Intercambio de Protección de Identidad.

INTERCAMBIO DE PROTECCIÓN DE IDENTIDAD

N°	Iniciador	Dirección	Respondedor	Notas
(1)	HDR; SA; NONCE	=>		Comienzo SA-ISAKMP o negociación Proxy
(2)		<=	HDR; SA	SA básica acordada
(3)	HDR; KE; NONCE	=>		
(4)		<=	HDR; KE; NONCE	Clave generada (por el Iniciador y Respondedor)
(5)	HDR*; KE; IDii; AUTH	=>		Identidad del Iniciador Verificada por el Respondedor
(6)		<=	HDR*; IDir; AUTH	Identidad del Respondedor Verificada por el Iniciador, SA establecida

En el primer mensaje (1), el iniciador genera una propuesta que considera adecuada para proteger el tráfico en una situación dada. Las cargas, SA, la de la Propuesta, y la de Transformación son incluidas en la carga de la SA (con propósitos de notación).

En el segundo mensaje (2), el respondedor indica el conjunto de protección que ha aceptado con la SA, la Propuesta, y la Carga de Transformación. La política de seguridad local determinará la acción del respondedor si no se acepta el conjunto de protección propuesto. Una posible acción es la transmisión de una carga de Notificación como parte de un Intercambio Informativo.

En el tercer (3) y cuarto (4) mensaje, el iniciador y el respondedor, respectivamente intercambian material clave usado para llegar a un secreto común compartido y la información aleatoria que es usada para garantizar la vida de la conexión y proteger contra ataques de reenvío. La información aleatoria proporcionada por ambas partes DEBERÍA ser usada por el mecanismo de autentificación para proporcionar prueba compartida de la participación en el intercambio. La política de seguridad local dictaminará la acción ha seguir si un error ocurre durante estos mensajes. Una posible acción es la transmisión de una carga de Notificación como parte de un Intercambio Informativo.

En el quinto (5) y sexto (6) mensaje, el iniciador y el respondedor, respectivamente, intercambian información de identificación y los resultados de la función de autentificación acordada. Esta información es trasmitida bajo la protección de un secreto común compartido. La política de seguridad local dictaminará la acción a seguir si ocurre un error durante estos mensajes. Una posible acción es la transmisión de una carga de Notificación como parte de un Intercambio Informativo.

4.6 Intercambio de Solamente Autentificación

El Intercambio de Solamente Autentificación está diseñado para permitir solamente la Autentificación relacionada con la información ha trasmitir. El beneficio de este intercambio es la capacidad de realizar solamente la autentificación sin otro costo computacional de claves. Usando este intercambio durante la negociación, ninguna información trasmitida será encriptada. Sin embargo, la información puede ser encriptada en otros lugares. Por ejemplo, si la encriptación es negociada durante la Fase 1 de una negociación y solamente el intercambio de autentificación es usado en la Fase 2 de la negociación, solamente el intercambio de autentificación será encriptado por la SAs de ISAKMP negociadas en la Fase 1. El siguiente diagrama muestra los mensajes con las posibles cargas enviadas en cada mensaje y las notas de ejemplo de un Intercambio de Solamente Autentificación.

INTERCAMBIO DE SOLAMENTE AUTENTIFICACIÓN

N°	Iniciador	Dirección	Respondedor	Notas
(1)	HDR; SA; NONCE	=>		Comienzo SA-ISAKMP o negociación Proxy
(2)		<=	HDR; SA; NONCE; IDir; AUTH	SA básica acordada, Identidad del Respondedor verificada por el Iniciador
(3)	HDR; IDii; AUTH	=>		Identidad del Iniciador verificada por el Respondedor, SA establecida

En el primer mensaje (1), el iniciador genera una propuesta que considera adecuada para proteger el tráfico en una situación dada. Las cargas, SA, la de la Propuesta, y la de Transformación están incluidas en la carga SA (para propósitos de notación). La información aleatoria que es usada para garantizar la vida de la conexión y proteger, contra ataques de reenvío también es trasmitida. La información aleatoria proporcionada por ambas partes DEBERÍA ser usada por el mecanismo de autentificación para proporcionar prueba compartida de la participación en el intercambio.

En el segundo (2) mensaje, el respondedor indica el conjunto de protección que ha aceptado con las cargas, SA, la de la Propuesta, y la de Transformación. Una vez más, la información aleatoria que es usada para garantizar la vida de la conexión y la protección contra ataques de reenvío también es trasmitida. La información aleatoria proporcionada por ambas partes DEBERÍA ser usada por el mecanismo de autentificación para proporcionar prueba compartida de la participación en el intercambio. Además, el respondedor debe transmitir información de identificación. Toda esta información es trasmitida bajo la protección de la función de autentificación acordada. La política de seguridad local dictaminará la acción del respondedor si no se acepta el conjunto de protección propuesto. Una posible acción es la transmisión de una carga de Notificación como parte de un Intercambio Informativo.

En el tercer (3) mensaje, el iniciador trasmite la información de identificación. Esta información es trasmitida bajo la protección de una función de autentificación acordada. La política de seguridad local dictaminará la acción ha seguir si un error ocurre durante estos mensajes. Una posible acción es la transmisión de una carga de Notificación como parte de un Intercambio Informativo.

4.7 Intercambio Agresivo

El Intercambio Agresivo está diseñado para permitir que la SA, el Intercambio de Claves y las cargas relacionadas con la Autentificación sean trasmitidas en forma simultánea. Combinar la SA, el intercambio de claves, y la información relacionada con la Autentificación en un mensaje, reduce el número de viajes de ida y vuelta a expensas de no proporcionar la protección de identidad. La protección de identidad no es proporcionada porque las identidades se intercambian antes de que un secreto común compartido haya sido establecido, por consiguiente, la encriptación de las identidades no es posible. Además, el Intercambio Agresivo es un intento para establecer toda la información relevante a la seguridad en un único intercambio. El siguiente diagrama muestra los mensajes con las posibles cargas enviadas en cada mensaje y las notas de ejemplo de un Intercambio Agresivo.

INTERCAMBIO AGRESIVO

N°	Iniciador	Dirección	Respondedor	Notas
(1)	HDR; SA; KE; NONCE; IDii	=>		Comienzo SA-ISAKMP o negociación Proxy y Intercambio de Claves
(2)		<=	HDR; SA; KE; NONCE; IDir; AUTH	Identidad del Iniciador verificada por el Respondedor, Clave generada, SA básica acordada
(3)	HDR*; AUTH	=>		Identidad del Respondedor verificada por el Iniciador, SA establecida

En el primer mensaje (1), el iniciador genera una propuesta que considera adecuada para proteger el tráfico para la situación dada. La SA, la Propuesta y las cargas de Transformación se incluyen en la carga de SA (para propósitos de notación). Solamente puede existir una Propuesta y una Transformación ofrecida (es decir no hay elección) acordada para el funcionamiento del intercambio agresivo. El material clave usado para llegar a un secreto común compartido y la información aleatoria que es usada para garantizar la vida de la conexión y protección contra ataques de reenvío también es trasmitida. La información aleatoria proporcionada por ambas partes DEBERÍA ser usada por el mecanismo de autentificación para proporcionar prueba compartida de la participación en el intercambio. Además, el iniciador trasmite información de identificación.

En el segundo (2) mensaje, el respondedor indica el conjunto de protección que ha aceptado con las cargas, SA, la de la Propuesta, y la de Transformación. El material clave usado para llegar a un secreto común compartido y la información aleatoria que es usada para garantizar la vida de la conexión y proteger contra ataques de reenvío también es transmitida. La información aleatoria proporcionada por ambas partes debe ser usada por el mecanismo de autentificación para proporcionar prueba compartida de la participación en el intercambio. Además, el respondedor trasmite la información de identificación. Toda esta información es trasmitida bajo la protección de una función de autentificación acordada. La política de seguridad local dictaminará la acción del respondedor si el conjunto de protección propuesto no es aceptado. Una posible acción es la transmisión de una carga de Notificación como parte de un Intercambio Informativo.

En el tercer (3) mensaje, el iniciador trasmite los resultados de la función de autentificación acordada. Esta información es trasmitida bajo la protección de un secreto común compartido. La política de seguridad local dictaminará la acción ha seguir si ocurre un error durante estos mensajes. Una posible acción es la transmisión de una carga de Notificación como parte de un Intercambio Informativo.

4.8 Intercambio Informativo

El Intercambio Informativo está diseñado como una transmisión de un solo sentido de la información que puede ser usada para la administración de una SA. El siguiente diagrama muestra los mensajes con las posibles cargas enviadas en cada mensaje y las notas de ejemplo de un Intercambio Informativo.

INTERCAMBIO INFORMATIVO

N°	Iniciador	Dirección	Respondedor	Notas
(1)	HDR*; N/D	=>		Notificación de Error o Cancelación

En el primer mensaje (1), el iniciador o el respondedor transmite una Notificación ISAKMP o una carga de Cancelación.

Si el Intercambio Informativo ocurre antes que el Intercambio de material clave, durante la Fase 1 de la negociación de ISAKMP, no habrá protección para el Intercambio Informativo. Una vez que el material clave haya sido intercambiado o una SA ISAKMP haya sido establecida, el Intercambio Informativo DEBE ser trasmitido bajo la protección proporcionada por el material clave o la SA ISAKMP.

Todos los intercambios son similares, en que en el comienzo de cada intercambio, la sincronización criptográfica DEBE ocurrir. El Intercambio Informativo es un intercambio y no un mensaje ISAKMP. Por ende, la generación de un Identificador de Mensaje (MID) para un Intercambio Informativo DEBERÍA ser independiente de los IVs o de otras comunicaciones en curso. Esto asegura que la sincronización de la criptografía es mantenida para las comunicaciones existentes y el Intercambio Informativo será procesado correctamente. La única excepción a esto es cuando el Bit de Commit de la cabecera de ISAKMP está en uno. Cuando el Bit de Commit está en uno, el campo Identificador de Mensaje del Intercambio Informativo DEBE contener el Identificador de Mensaje de la negociación de la SA de la Fase 2 de ISAKMP primitiva, en vez de un nuevo Identificador de Mensaje (MID). Esto se realiza para asegurar que el Intercambio Informativo está vinculado con el Mensaje de Notificación pudiendo ser asociado con la correcta Fase 2 de la SA. Para una descripción del Bit de Commit véase la Sección 3.1

5 Procesamiento de la Carga ISAKMP

La Sección 3 describe las cargas de ISAKMP. Estas cargas son usadas en los intercambios descriptos en la Sección 4 y pueden ser usados en los intercambios para DOI específicos. Esta sección describe el procesamiento para cada una de las cargas. Esta sección sugiere registrar eventos en un sistema de auditoría de archivos. Esta acción es controlada por una política de sistemas de seguridad y por lo tanto es una acción sugerida.

5.1 Procesamiento General del Mensaje

Cada mensaje ISAKMP tiene un procesamiento básico aplicado para asegurar la confiabilidad del protocolo, y para minimizar amenazas, tales como denegación de servicio y ataques de reenvío. Todos los procesamientos DEBERÍAN incluir chequeos de la longitud del paquete para asegurar que el paquete recibido tiene la longitud dada en la cabecera de ISAKMP. Si la longitud del mensaje ISAKMP y el valor en el campo de longitud de la carga en la cabecera de ISAKMP no son los mismos, el mensaje ISAKMP DEBE ser rechazado. La entidad receptora (iniciador o respondedor) DEBE hacer lo siguiente:

1. El evento, LONGITUD DE LAS CARGAS DESIGUALES, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

2. Un Intercambio Informativo con una carga de Notificación conteniendo el mensaje, LONGITUD DE CARGA DESIGUAL, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de política de seguridad.

Al trasmitir un mensaje ISAKMP, la entidad transmisora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Fijar el timer y inicializar un retry counter.

   NOTA: las implementaciones NO DEBEN usar un valor de timer prefijado. En lugar de esto los valores del timer de transmisión deben ser ajustados dinámicamente basados en el tiempo de ida y vuelta. Además, sucesivas retransmisiones del mismo paquete deben estar separadas por intervalos de tiempo cada vez más largos (por ejemplo cuando un host que ha experimentado una colisión en una red espera un tiempo exponencial para retransmitir).

2. Si el timer espira, el mensaje ISAKMP es reenviado y el retry counter es decrementado.

3. Si el retry counter llega a cero (0), el evento, ALCANZÓ EL LIMITE DE REINTENTOS, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

4. El mecanismo del protocolo ISAKMP borra todos los estados y retorna a un estado INACTIVO.

5.2 Procesamiento de la Cabecera ISAKMP

Cuando se crea un mensaje ISAKMP, la entidad transmisora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Crear la cookie respectiva. Ver Sección 2.5.3 para más detalles.

2. Determinar las características de seguridad relevantes de la sesión (es decir el DOI y situación).

3. Construir una Cabecera ISAKMP con los campos descriptos en la Sección 3.1.

4. Construir otras cargas ISAKMP, dependiendo del tipo de intercambio.

5. Trasmitir el mensaje al host de destino como se describe en la Sección 5.1.

Cuando un mensaje ISAKMP es recibido, la entidad receptora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Verificar la "cookies" del iniciador y del respondedor. Si la validación de la cookie falla, el mensaje es descartado y las siguientes acciones son tomadas:

(a) El evento, COOKIE NO VÁLIDA, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

(b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, COOKIE NO VÁLIDA, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

2. Comprobar el Campo Carga Siguiente para confirmar si es válido. Si la validación del campo Carga Siguiente falla, el mensaje es descartado y las siguientes acciones son tomadas:

(a) El evento, CARGA SIGUIENTE NO VÁLIDA, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

(b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, TIPO DE CARGA NO VÁLIDO, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

3. Comprobar el campo Versión Mayor y el campo Versión Menor para confirmar si son los correctos (ver Sección 3.1). Si la validación del campo de la versión falla, el mensaje es descartado y las siguientes acciones son tomadas:

(a) El evento, VERSIÓN ISAKMP NO VÁLIDA, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

(b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, VERSIÓN MAYOR NO VÁLIDA o VERSIÓN MENOR NO VÁLIDA, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

4. Comprobar el campo Tipo de Intercambio para confirmar si es válido. Si la validación del campo Tipo de Intercambio falla, el mensaje es descartado y las siguientes acciones son tomadas:

(a) El evento, TIPO DE INTERCAMBIO NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

(b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, TIPO DE INTERCAMBIO NO VÁLIDO, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

5. Comprobar el campo Banderas para asegurarse de que contienen los valores correctos. Si la validación del campo Banderas falla, el mensaje es descartado y las siguientes acciones son tomadas:

   (a) El evento, BANDERAS NO VALIDAS, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, BANDERAS NO VALIDAS, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

6. Comprobar el campo Identificador de Mensaje para asegurarse que contiene los valores correctos. Si la validación del Identificador de Mensaje falla, el mensaje es descartado y las siguientes acciones son tomadas:

   (a) El evento, IDENTIFICADOR DE MENSAJE NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, IDENTIFICADOR DE MENSAJE NO VÁLIDO, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

7. El procesamiento del mensaje ISAKMP continúa usando el valor del campo Carga Siguiente.

5.3 Procesamiento de la Cabecera de Carga Genérica

Cuando se crea cualquiera de las Cargas ISAKMP descriptas desde la Sección 3.4 hasta la Sección 3.15 una Cabecera de Carga Genérica es colocada al comienzo de estas cargas. Al crear una Cabecera de Carga Genérica, la entidad transmisora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Colocar el valor de la Carga Siguiente en el campo de Carga Siguiente. Estos valores están descriptos en la Sección 3.1.

2. Colocar el valor cero (0), en el campo RESERVADO.

3. Colocar la longitud (en octetos) de la carga en el campo Longitud de la Carga.

4. Construir las cargas según lo definido en el resto de esta sección.

Cuando se reciben cualquiera de las cargas ISAKMP, la entidad receptora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Comprobar el campo Carga Siguiente para confirmar si es válido. Si la validación del campo Carga Siguiente falla, el mensaje es descartado y las siguientes acciones son tomadas:

   (a) El evento, CARGA SIGUIENTE NO VÁLIDA, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, TIPO DE CARGA NO VÁLIDA, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

2. Comprobar que el campo RESERVADO contenga el valor cero. Si el valor en el campo RESERVADO no es cero, el mensaje es descartado y las siguientes acciones son tomadas:

   (a) El evento, CAMPO RESERVADO NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, SINTAXIS DE LA PROPUESTA DEFICIENTE o CARGA MAL FORMADA, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

3. Procesar las cargas restantes según lo definido por el campo Carga Siguiente.

5.4 Procesamiento de la Carga SA

Cuando se crea una carga SA, la entidad transmisora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar el Dominio de Interpretación para el cual se está realizando esta negociación.

2. Determinar la situación dentro del DOI determinado para el cual se está realizando esta negociación.

3. Determinar las propuesta(s) y las transformación(es) dentro de la situación. Estas están descriptas en las Secciones 3.5 y 3.6 respectivamente.

4. Construir una carga SA.

5. Trasmitir el mensaje a la entidad receptora como se describe en la Sección 5.1.

Cuando una carga SA es recibida, la entidad receptora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar si el Dominio de Interpretación (DOI) es soportado. Si la determinación del DOI falla, el mensaje es descartado y las siguientes acciones son tomadas:

   (a) El evento, DOI NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, DOI NO SOPORTADO, DEBE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

2. Determinar si la Situación dada puede ser protegida. Si la determinación de la Situación falla, el mensaje es descartado y las siguientes acciones son tomadas:

   (a) El evento, SITUACIÓN NO VÁLIDA, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, SITUACIÓN NO SOPORTADA, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

3. Procesar las cargas restantes (es decir, la carga de la Propuesta y la de Transformación) a la de la carga SA.. Si la Propuesta de la SA (como se describe en las Secciones 5.5 y 5.6) no es aceptada, la siguientes acciones son tomadas:

   (a) El evento, PROPUESTA NO VÁLIDA, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, ELECCIÓN DE LA PROPUESTA NO VÁLIDA, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

5.5 Procesamiento de la Carga de la Propuesta

Cuando se crea una Carga de la Propuesta la entidad transmisora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar el Protocolo para esta propuesta.

2. Determinar el número de propuestas que serán ofrecidas para este protocolo y el número de trasformaciones para cada propuesta. Las trasformaciones están descritas en la Sección 3.6.

3. Generar un único SPI seudo aleatorio.

4. Construir una carga de la Propuesta.

Cuando una carga de Propuesta es recibida, la entidad receptora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar si el Protocolo es soportado. Si el campo Identificador de Protocolo no es válido, la carga es descartada y las siguientes acciones son tomadas:

   (a) El evento, PROTOCOLO NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, IDENTIFICADOR DE PROTOCOLO NO VÁLIDO, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

2. Determinar si el SPI es válido. Si el SPI no es válido, la carga es descartada y las siguientes acciones son tomadas:

   (a) El evento, SPI NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, SPI NO VÁLIDO, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de política de seguridad.

3. Asegurar que la Propuestas estén presentadas conforme a los detalles dados en las Secciones 3.5 y 4.2. Si las propuestas no están formuladas correctamente las siguientes acciones son tomadas:

   (a) Los posibles eventos, SINTAXIS DE LA PROPUESTA DEFICIENTE, PROPUESTA NO VÁLIDA, PUEDEN ser registrados en un apropiado sistema de auditoría de archivos.

(b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, SINTAXIS DE LA PROPUESTA DEFICIENTE o CARGA MAL FORMADA, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

4. Procesar las cargas de la Propuesta y Transformación según lo definido por el campo Carga Siguiente. Ejemplos del procesamiento de estas cargas están dados en la Sección 4.2.1.

5.6 Procesamiento de la Carga de Transformación

Cuando se crea una Carga de Transformación, la entidad transmisora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar el número de Transformación para esta transformación.

2. Determinar el número de trasformaciones que serán ofrecidas para esta propuesta. Las Trasformaciones se describen en la Sección 3.6.

3. Construir una Carda de Transformación.

Cuando una carga de Transformación es recibida, la entidad receptora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar si la Transformación es soportada. Si el campo Identificador de Transformación contiene un valor no conocido o no soportado, la carga de Transformación DEBE ser ignorada y NO DEBE causar la generación de un evento de TRANSFORMACIÓN NO VÁLIDA. Si el campo Identificador de Transformación no es válido, la carga es descartada y las siguientes acciones son tomadas:

   (a) El evento, TRASFORMACIÓN NO VÁLIDA, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, IDENTIFICADOR DE TRANSFORMACIÓN NO VÁLIDO, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

2. Asegurar que las Trasformaciones estén presentadas conforme a los detalles dados en las Secciones 3.6 y 4.2. Si las transformaciones no están formuladas correctamente, las siguientes acciones son tomadas:

(a) Los posibles eventos, SINTAXIS DE LA PROPUESTA DEFICIENTE, TRANSFORMACIÓN NO VÁLIDA, ATRIBUTOS NO VALIDOS, son registrados en un apropiado sistema de auditoría de archivos.

(b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, SINTAXIS DE LA PROPUESTA DEFICIENTE, CARGA MAL FORMADA o ATRIBUTOS NO SOPORTADOS, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

3. Procesar las cargas de Transformación y Propuestas subsiguientes, según lo definido por el campo Carga Siguiente. Ejemplos del procesamiento de estas cargas están dados en la Sección 4.2.1.

5.7 Procesamiento de la Carga de Intercambio de Claves

Cuando se crea una Carga de Intercambio de Claves la entidad transmisora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar el Intercambio de Claves que será utilizado como lo define el DOI.

2. Determinar el uso del campo de Datos de Intercambio de Claves como lo define el DOI.

3. Construir una carga de Intercambio de Claves.

4. Trasmitir el mensaje a la entidad receptora como se describe en la Sección 5.1.

Cuando una carga de Intercambio de Claves es recibida, la entidad receptora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar si el Intercambio de Claves es soportado. Si la determinación del intercambio de claves falla, el mensaje es descartado y las siguientes acciones son tomadas:

(a) El evento, INFORMACIÓN DE CLAVE NO VÁLIDA, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

(b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, INFORMACIÓN DE CLAVE NO VÁLIDA, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

5.8 Procesamiento de la Carga de Identificación

Cuando se crea una Carga de Identificación, la entidad transmisora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar la información de Identificación que será usada según lo definido por el DOI (y posiblemente la situación).

2. Determinar el uso del campo de Datos de Identificación según lo definido por el DOI.

3. Construir una carga de Identificación.

4. Trasmitir el mensaje a la entidad receptora como se describe en la Sección 5.1.

Cuando una carga de Identificación es recibida, la entidad receptora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar si el Tipo de Identificación es soportado. Esto puede estar basado en el DOI y la Situación. Si la determinación de Identificación falla, el mensaje es descartado y las siguientes acciones son tomadas:

   (a) El evento, INFORMACIÓN DEL IDENTIFICADOR NO VÁLIDA, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, INFORMACIÓN DEL IDENTIFICADOR NO VÁLIDO, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

5.9 Procesamiento de la Carga de Certificado

Cuando se crea una Carga de Certificado, la entidad transmisora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar la Codificación de Certificación que será usada. Esto puede estar especificado por el DOI.

2. Asegurar la existencia del certificado formateado según lo definido en la Codificación del Certificado.

3. Construir una carga de Certificado.

4. Trasmitir el mensaje a la entidad receptora como se describe en la Sección 5.1.

Cuando una Carga de Certificado es recibida, la entidad receptora (iniciador o respondedor) debe hacer lo siguiente:

1. Determinar si la Codificación de Certificación es soportada. Si la Codificación de Certificación no es soportada, la carga es descartada y las siguientes acciones son tomadas:

   (a) El evento, TIPO CERTIFICACIÓN NO VÁLIDA, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, CODIFICACIÓN DE CERTIFICACIÓN NO VÁLIDO, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

2. Procesar el campo Datos del Certificados. Si los Datos Certificados no son válidos o está formateado inapropiada mente, la carga es descartada y las siguientes acciones son tomadas:

   (a) El evento, CERTIFICADO NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, CERTIFICADO NO VÁLIDO, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

5.10 Procesamiento de la Carga de Solicitud de Certificado

Cuando una Carga de Solicitud de Certificado se crea, la entidad transmisora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar el tipo de Codificación de Certificación que será solicitado. Esto puede estar especificado por el DOI.

2. Determinar el nombre de una Autoridad de Certificación (CA) aceptable a la cual se le solicitará (si es aplicable).

3. Construir una carga de Solicitud de Certificado.

4. Trasmitir el mensaje a la entidad receptora como se describe en la Sección 5.1.

Cuando la Carga de Solicitud de Certificado es recibida, la entidad receptora (iniciador o respondedor) debe hacer lo siguiente:

1. Determinar si la Codificación de Certificación es soportada. Si la Codificación de Certificación no es válida, la carga es descartada y las siguientes acciones son tomadas:

   (a) El evento, TIPO DE CERTIFICACIÓN NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, CODIFICACIÓN DE CERTIFICADO NO VÁLIDO, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

   Si la Codificación de Certificación no es soportada, la carga es descartada y las siguientes acciones son tomadas:

   (a) El evento, TIPO DE CERTIFICACIÓN NO SOPORTADO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, TIPO DE CERTIFICACIÓN NO SOPORTADO, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

2. Determinar si la Autoridad de Certificación es soportada por la Codificación de Certificación especificada. Si la Autoridad de Certificación no es válida o es formateada inapropiadamente, la carga es descartada y las siguientes acciones son tomadas:

   (a) El evento, AUTORIDAD DE CERTIFICACIÓN NO VÁLIDA, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, AUTORIDAD DE CERTIFICACIÓN NO VÁLIDA, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

3. Procesar la Solicitud de Certificación. Si un Tipo de Certificado solicitado con una Autoridad de Certificación especifica no está disponible, la carga es descartada y las siguientes acciones son tomadas:

(a) El evento, CERTIFICACIÓN NO DISPONIBLE, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

(b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, CERTIFICACIÓN NO DISPONIBLE, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

5.11 Procesamiento de la Carga Hash

Cuando una Carga Hash es creada la entidad transmisora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar la función Hash que será usada según lo definido por la negociación de la SA.

2. Determinar el uso del campo Datos Hash según lo definido por el DOI.

3. Construir una carga Hash.

4. Trasmitir el mensaje a la entidad receptora según lo descripto en la Sección 5.1.

Cuando una carga Hash es recibida, la entidad receptora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar si el Hash es soportado. Si la determinación del hash falla, el mensaje es descartado y las siguientes acciones son tomadas:

   (a) El evento, INFORMACIÓN DE HASH NO VÁLIDA, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, INFORMACIÓN DE HASH NO VÁLIDO, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

2. Realizar la función de Hash como se explicó en el DOI y/o en los documentos de los protocolos de Intercambio de Claves. Si la función Hash falla, el mensaje es descartado y las siguientes acciones son tomadas:

   (a) El evento, VALOR DE HASH NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

(b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, ERROR EN LA AUTENTIFICACIÓN, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

5.12 Procesamiento de la Carga de la Firma

Cuando se crea una Carga de Firma, la entidad transmisora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar la función de la Firma que será usada según lo definido por la negociación de la SA.

2. Determinar el uso del campo Datos de la Firma según lo definido por el DOI.

3. Construir la carga de la Firma.

4. Trasmitir el mensaje a la entidad receptora como se describió en la Sección 5.1.

Cuando una carga de Firma es recibida la entidad receptora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar si la Firma es soportada. Si la determinación de la Firma falla el mensaje es descartado y las siguientes acciones son tomadas:

   (a) El evento, INFORMACIÓN DE LA FIRMA NO VÁLIDA, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, FIRMA NO VÁLIDA, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

2. Realizar la Función de la firma conforme al DOI y/o los documentos del protocolo de Intercambio de Claves. Si la función de la Firma falla el mensaje es descartado y las siguientes acciones son tomadas:

   (a) El evento, VALOR DE LA FIRMA NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

   (b) Un Intercambio Informativo con una carga de Notificación conteniendo el tipo de mensaje, ERROR EN LA AUTENTIFICACIÓN, PUEDE ser enviado a la entidad transmisora. Esta acción es dictaminada por un sistema de políticas de seguridad.

5.13 Procesamiento de la Carga Nonce

Cuando se crea una carga Nonce, la entidad transmisora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Crear un valor aleatorio único que será usado como un nonce.

2. Construir una carga Nonce.

3. Trasmitir el mensaje a la entidad receptora como se describe en la Sección 5.1.

Cuando una carga Nonce es recibida, la entidad receptora (iniciador o respondedor) DEBE hacer lo siguiente:

1. No hay procesamientos específicos para el procesamiento de cargas nonces. Los procedimientos están definidos por el tipo de intercambio (y posiblemente por el DOI y las descripciones del intercambio de claves).

5.14 Procesamiento de la Carga de Notificación

Durante las comunicaciones es posible que puedan ocurrir errores. El Intercambio Informativo con una Carga de Notificación proporciona un método controlado para informar a una entidad usuaria que errores se han producido durante el procesamiento. Se RECOMIENDA que las Cargas de Notificación sean enviadas en un Intercambio Informativo separado en lugar de anexarlas a una Carga de Notificación de un intercambio existente.

Cuando se crea una Carga de Notificación, la entidad transmisora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar el DOI para esta Notificación.

2. Determinar el Identificador del Protocolo para esta Notificación.

3. Determinar el tamaño del SPI basándose en el campo Identificador de Protocolo. Este campo es necesario porque diferentes protocolos de seguridad tienen diferentes tamaños de SPI. Por ejemplo, ISAKMP combina el par de cookies del Iniciador y el Respondedor (16 octetos) como un SPI, mientras que ESP y AH tienen SPIs de 4 octetos.

4. Determinar el Tipo de Mensaje de Notificación basándose en el error o en el estado del mensaje deseado.

5. Determinar el SPI que se asocia con esta notificación.

6. Determinar si los Datos de Notificación adicional serán incluidos. Esto es información adicional especificada por el DOI.

7. Construir una carga de Notificación.

8. Trasmitir el mensaje a la entidad receptora como se describe en la Sección 5.1.

Debido a que un Intercambio Informativo con una carga de Notificación es un mensaje unidireccional, una retransmisión no será realizada. La política de seguridad local dictaminará los procedimientos a seguir. Sin embargo, nosotros RECOMENDAMOS que un evento, ERROR DE CARGA DE NOTIFICACIÓN, sea registrado en un apropiado sistema de auditoría de archivos por la entidad receptora.

Si un Intercambio Informativo ocurre antes del intercambio de material clave durante la primera fase de la negociación de ISAKMP no habrá protección proporcionada para el Intercambio Informativo. Una vez que el material clave ha sido intercambiado o la SA ISAKMP ha sido establecida, el Intercambio Informativo DEBE ser trasmitido bajo la protección proporcionada por el material clave o la SA ISAKMP.

Cuando una carga de Notificación es recibida, la entidad receptora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar si el Intercambio Informativo tiene alguna protección aplicada por medio de la comprobación del Bit de Encriptación y del Bit de Solo Autentificación en la cabecera de ISAKMP. Si el Bit de Encriptación está fijado, es decir el Intercambio Informativo es encriptado, el mensaje DEBE ser desencriptado usando la (en proceso o ya establecida) SA ISAKMP. Una vez que la desencriptación es completada el proceso puede continuar como se describe abajo. Si el Bit de Solo Autentificación esta fijado, el mensaje DEBE ser autentificado usando la (en proceso o ya establecida) SA ISAKMP. Una vez que la autentificación es completada, el proceso puede continuar como se describe debajo. Si el Intercambio Informativo no es encriptado o autentificado, el procesamiento de la carga puede continuar como se describe debajo.

2. Determinar si el DOI es soportado. Si la determinación del DOI falla, la carga es descartada y la siguiente acción es tomada:

   (a) El evento, DOI NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

3. Determinar si el Identificador de Protocolo es soportado. Si la determinación del Identificador de Protocolo falla, la carga es descartada y la siguiente acción es tomada:

   (a) El evento, IDENTIFICADOR DE PROTOCOLO NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

4. Determinar si el SPI es válido. Si el SPI no es válido, la carga es descartada y la siguiente acción es tomada:

   (a) El evento, SPI NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

5. Determinar si el Tipo de Mensaje de Notificación es válido. Si el Tipo de Mensaje de Notificación no es válido, la carga es descartada y la siguiente acción es tomada:

   (a) El evento, TIPO DE MENSAJE NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

6. Procesar la carga de Notificación, incluyendo los Datos de Notificación adicional y tomar la acción apropiada, de acuerdo con la política de seguridad local.

5.15 Procesamiento de la Carga de Cancelación

Durante las comunicaciones es posible que hosts puedan estar comprometidos o que la información pueda ser interceptada durante la transmisión. La determinación de que esto ha ocurrido no es una tarea fácil y esta fuera del alcance de este documento. Sin embargo si se descubre que las trasmisiones son comprometidas, es necesario establecer una nueva SA y cancelar la actual.

El Intercambio Informativo con una Carga de Cancelación proporciona un método controlado de informar a una entidad usuaria de que la entidad transmisora a cancelado la SA(s). La cancelación de SA siempre DEBE ser realizada bajo la protección de una SA ISAKMP. La entidad receptora DEBERÍA limpiar la base de datos de SA local. Sin embargo, bajo el recibo de un mensaje de Cancelación las SAs enumeradas en el campo SPI de la carga de Cancelación no pueden ser usados con la entidad transmisora. El procedimiento de establecimiento de SA debe ser invocado para el restablecimiento de comunicaciones seguras.

Cuando se crea una Carga de Cancelación, la entidad transmisora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Determinar el DOI para esta cancelación.

2. Determinar el Identificador de Protocolo para esta cancelación.

3. Determinar el tamaño del SPI basado en el campo Identificador de Protocolo. Este campo es necesario porque, diferentes protocolos de seguridad tienen diferentes tamaños de SPI. Por ejemplo, ISAKMP combina el par de cookies del iniciador y del respondedor (16 octetos) como un SPI, mientras que ESP y AH tienen SPIs de 4 octetos.

4. Determinar el número de SPIs que serán cancelados para este protocolo.

5. Determinar el o los SPI(s) que serán asociados con esta cancelación.

6. Construir una carga de Cancelación.

7. Trasmitir el mensaje a la entidad receptora como se describe en la Sección 5.1.

Debido a que un Intercambio Informativo con una carga de cancelación es un mensaje unidireccional una retransmisión no será realizada. La política de seguridad local determinará el procedimiento a seguir. Nosotros RECOMENDAMOS que un evento de ERROR DE CARGA DE CANCELACIÓN sea registrado en un apropiado sistema de auditoría de archivos por la entidad receptora.

Como se describió anteriormente, un Intercambio Informativo con una carga de Cancelación DEBE ser trasmitido bajo la protección proporcionada por una SA ISAKMP.

Cuando una carga de Cancelación es recibida, la entidad receptora (iniciador o respondedor) DEBE hacer lo siguiente:

1. Debido a que el Intercambio Informativo está protegido por un cierto servicio de seguridad (por ejemplo autentificación para una SA de Solo Autentificación, encriptación para otros intercambios), el mensaje DEBE tener estos servicios de seguridad aplicados usando la SA ISAKMP. Una vez que el procesamiento del servicio de seguridad es completado el procesamiento puede continuar como se describe debajo. Cualquier error que ocurra durante el procesamiento del servicio de seguridad será evidente al controlar la información en la carga de Cancelación. La política de seguridad local DEBERÍA dictaminar cualquier acción a seguir como resultado de errores en el procesamiento del servicio de seguridad.

2. Determinar si el DOI es soportado. Si la determinación del DOI falla, la carga es descartada y las siguiente acción es tomada:

   (a) El evento, DOI NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

3. Determinar si el Identificador de Protocolo es soportado. Si la determinación del Identificador de Protocolo falla, la carga es descartada y la siguiente acción es tomada:

   (a) El evento, IDENTIFICADOR DE PROTOCOLO NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

4. Determinar si el SPI es válido para cada SPI incluido en la carga de Cancelación. Para cada SPI que no sea válido, la siguiente acción es tomada:

   (a) El evento, SPI NO VÁLIDO, PUEDE ser registrado en un apropiado sistema de auditoría de archivos.

5. Procesar la carga de Cancelación y tomar una acción apropiada, de acuerdo con la política de seguridad local. Como se describió anteriormente, una acción apropiada DEBERÍA incluir la limpieza de la base de datos de la SA local.

6 Conclusiones

El Protocolo de Gestión de Claves y Asociaciones de Seguridad en Internet (ISAKMP) es un protocolo bien diseñado que apunta a la Internet del Futuro. El crecimiento masivo de Internet conducirá a una gran diversidad de la utilización de la red, comunicaciones, requerimientos de seguridad, y mecanismos de seguridad. ISAKMP contiene todas las características que serán necesarias para ese ambiente de comunicaciones dinámico y amplio.

La característica de SA ISAKMP junto con la autentificación y el establecimiento de claves proporcionan la seguridad y flexibilidad que serán necesarias para la diversidad y crecimiento futuro. Esta diversidad de seguridad de múltiples técnicas de intercambio de claves, algoritmos de encriptación, mecanismos de autentificación, servicios de seguridad, y atributos de seguridad permitirán a los usuarios seleccionar la seguridad apropiada para sus redes, comunicaciones, y necesidades de seguridad. El uso de las características de SA permite especificar y negociar requerimientos de seguridad con otros usuarios. Un beneficio adicional de soportar múltiples técnicas en un único protocolo es que a medida que nuevas técnicas son desarrolladas pueden ser fácilmente agregadas al protocolo, esto proporciona un camino para el crecimiento de los

servicios de seguridad de Internet. ISAKMP soporta SAs definidas públicas y privadamente, haciéndolas ideal para el gobierno, comercio y comunicaciones privadas.

ISAKMP proporciona la capacidad de establecer SAs para múltiples protocolos de seguridad y aplicaciones. Estos protocolos o aplicaciones pueden estar o no orientados a sesiones. Teniendo un protocolo para el establecimiento de SAs que soporte múltiples protocolos de seguridad elimina la necesidad de múltiples, autentificaciones similares, intercambios de claves y protocolos de establecimientos de SAs cuando más de un Protocolo de seguridad está en uso o es requerido. Así como IP proporciona la capa de red común para la Internet un protocolo de establecimiento de seguridad común es necesario para que la seguridad se convierta en una realidad en Internet. ISAKMP proporciona la base común que permite a todos los otros protocolos de seguridad ínter operar.

ISAKMP sigue buenos principios de diseño de seguridad. No está vinculado a otros protocolos de trasporte inseguros, por lo tanto no es vulnerable o debilitado por ataques a otros protocolos. También, cuando más protocolos de trasporte seguros son desarrollados, ISAKMP puede fácilmente emigrar con ellos. ISAKMP también proporciona protección contra ataques vinculados a protocolos. Esta protección proporciona seguridad de que las SAs y el establecimiento de claves están con la parte deseada y no con un atacante.

ISAKMP también sigue buenos principios de diseño de protocolo. La información específica del protocolo solo está en la cabecera del protocolo, siguiendo los principios de diseño de IPv6. Los datos trasportados por el protocolo están separados dentro de cargas funcionales. A medida que Internet crece y evoluciona, nuevas cargas para soportar nuevas funcionalidades de seguridad pueden ser agregadas sin modificar el protocolo entero.

A Atributos de una Asociación de Seguridad ISAKMP

A.1 Antecedentes/Fundamentos

Como está detallado en secciones previas, ISAKMP está diseñado para proporcionar un marco flexible y extensible para el establecimiento y la administración de SAs y claves criptográficas. Este marco proporcionado por ISAKMP consiste de definiciones de carga y cabeceras, de tipos de intercambio para guiar el mensaje y los intercambios de carga y las pautas generales de procesamiento. ISAKMP no define los mecanismos que serán usados para establecer y administrar las SAs y claves criptográficas en un modo autentificado y confidencial. La definición de mecanismos y sus aplicaciones son de la incumbencia de los Dominios de Interpretación (DOIs) individuales.

La definición de estos mecanismos es la articulación de DOI individuales.

Esta sección describe los valores de ISAKMP para el DOI de Seguridad IP en Internet, Protocolos de seguridad soportados, y valores de identificación para las negociaciones de la Fase 1 de ISAKMP. El DOI de Seguridad IP en Internet es OBLIGATORIO para las implementaciones de seguridad IP. [Oakley] y [IKE] describen, en detalle, los mecanismos y sus aplicaciones para el establecimiento y la administración de SAs y claves criptográficas para la seguridad IP.

A.2 Valor Asignado al DOI de Seguridad IP en Internet

Como se describe en [IPDOI], el número asignado al DOI de Seguridad IP en Internet es uno (1).

A.3 Protocolos de Seguridad Soportados

Los valores para los protocolos de seguridad soportados son especificados en los más recientes "números asignados" [STD-2]. Presentados en la siguiente tabla están los los valores de los protocolos de seguridad soportados por ISAKMP para el DOI de Seguridad IP en Internet.

Protocolo	Valor Asignado
Reservado	0
ISAKMP	1

Todos los DOIs DEBEN reservar ISAKMP con un identificador de protocolo de 1. Todos los otros protocolos de seguridad dentro del DOI serán enumerados consecuentemente.

Los valores del protocolo de seguridad de 2 hasta 15359 están reservados por la IANA para uso futuro. Los valores de 15360 hasta 16383 están permanentemente reservados para el uso privado entre implementaciones mutuamente acordadas. Tales valores de uso privado son poco probables de ser ínter operables a través de diferentes implementaciones.

A.4 Valores del Tipo de Identificación de ISAKMP

La tabla siguiente enumera los valores asignados al campo Tipo de Identificación encontrados en la carga de identificación durante un intercambio genérico de Fase 1, el cuál no es para un protocolo específico.

Tipo de Identificador	Valor
Identificador de dirección IPv4	0
Identificador de dirección de subred IPv4	1
Identificador de dirección IPv6	2
Identificador de dirección de subred IPv6	3

A.4.1 Identificador de Dirección IPv4

El tipo de Identificador de dirección IPv4 especifica un valor de cuatro (4) octetos para la dirección de IPv4.

A.4.2 Identificador de Dirección de Subred IPv4

El tipo de Identificador de dirección de subred para IPv4, especifica una serie de direcciones para IPv4, representado por dos valores de cuatro (4) octetos. El primer valor es una dirección IPv4, el segundo valor es una máscara de red IPv4. Note que unos en la máscara de red indican que el bit correspondiente en la dirección es fijo, mientras que los ceros indica un bit "comodín".

A.4.3 Identificador de Dirección IPv6

El tipo de identificador de dirección IPv6 especifica un valor de dieciséis (16) octetos para la dirección IPv6.

A.4.4 Identificador de Dirección de Subred IPv6

El tipo de Identificador de dirección de subred de IPv6, especifica una serie de direcciones para IPv6, representados por dos valores de dieciséis (16) octetos. El primer valor es una dirección IPv6 el segundo es una máscara de red IPv6. Note que los unos en la mascara de red indican que el bit correspondiente en la dirección es fijo, mientras que los ceros indican un bit "comodín".

B Definición de un Nuevo Dominio de Interpretación

El DOI de Internet puede ser suficiente para resolver los requerimientos de seguridad de una gran parte de la comunidad de Internet. Sin embargo algunos grupos pueden tener la necesidad de reformar algunos aspectos del DOI, tal vez agregar un conjunto de algoritmos criptográficos diferentes, o tal vez por que quieran tomar decisiones relevantes a la seguridad basados en algo más que un identificador de host o un identificador de usuario. También, un grupo particular puede tener la necesidad de un nuevo tipo de intercambio, como por ejemplo para soportar la administración de claves para grupos multicast.

Esta sección discute los lineamientos para la definición de un nuevo DOI. Una completa especificación del DOI de Internet puede ser encontrada en [IPDOI].

Definir un nuevo DOI es probable que sea un proceso que lleve mucho tiempo. En lo posible, se recomienda que el diseñador comience con un DOI existente y que modifique solamente las partes que son inaceptables.

Si un diseñador elige comenzar de cero, lo que sigue DEBE ser definido:

- Una "situación": El conjunto de información que será utilizado para determinar los servicios de seguridad requeridos.
- El conjunto de políticas de seguridad que debe ser soportado.
- Un esquema para nombrar información de seguridad relevante, incluyendo algoritmos de encriptación, algoritmos de intercambios de claves etc.
- Una sintaxis para la especificación de los servicios de seguridad propuestos, atributos, y autoridades de certificación.
- El formato específico para los contenidos de varias cargas.
- Tipos de intercambios adicionales, si son requeridos.

B.1 Situación

La situación es la base para decidir como proteger un canal de comunicaciones. Debe contener todos los datos que serán usados para determinar los tipos y las fuerzas de protección aplicadas a una SA. Por ejemplo el departamento de defensa de USA probablemente use algoritmos no publicados y tendría atributos adicionales especiales

que negociar. Estos atributos de seguridad adicionales estarían incluidos en la situación.

B.2 Políticas de Seguridad

Las políticas de seguridad definen como varios tipos de información deben estar clasificados y protegidos. El DOI debe definir el conjunto de políticas de seguridad soportado, por que ambas partes en una negociación deben confiar en que la otra parte comprende una situación, y protegerá la información apropiadamente, en tránsito y almacenada. En un ambiente corporativo, por ejemplo, ambas partes en una negociación deben acordar el significado del término "información privada" antes de que puedan negociar como protegerla.

Note que incluyendo las políticas de seguridad requeridas en el DOI solamente especifica que los hosts participantes entiendan e implementen aquellas políticas en un contexto de un sistema global.

B.3 Esquemas de Nombramiento

Cualquier DOI debe definir un modo consistente de nombrar algoritmos criptográficos, autoridades de certificación, etc. Esto puede ser usualmente realizado utilizando las convenciones de nombramiento de la IANA, talvez con algunas extensiones privadas.

B.4 Sintaxis para la Especificación de Servicios de Seguridad

Además de simplificar la especificación de cómo nombrar entidades, el DOI también debe especificar el formato completo de la propuesta de como proteger el tráfico bajo una determinada situación.

B.5 Especificación de Carga

El DOI debe especificar el formato para cada uno de los tipos de carga. Para varios tipos de carga, ISAKMP a incluido campos que tendrían que estar presentes a través de todo el DOI (tales como una autoridad de certificación en la carga de certificado, un identificador de intercambio de claves en la carga de intercambio de claves).

B.6 Definición de Nuevos Tipos de Intercambio

Si los tipos básicos de intercambio son inadecuados para resolver los requisitos dentro de un DOI, un diseñador puede definir hasta 13 tipos de intercambio extras por DOI. El diseñador crea un nuevo tipo de intercambio eligiendo un valor no usado de tipo de intercambio, y definiendo una secuencia de mensajes compuesta de encadenamientos de tipos de carga de ISAKMP.

Note que cualquiera de los nuevos tipos de intercambio debe ser rigurosamente analizado debido a vulnerabilidades. Puesto que esto es una tarea costosa e imprecisa, un nuevo tipo de intercambio debe ser creado si es absolutamente necesario.

Consideraciones de Seguridad

Las técnicas de análisis criptográficos están mejorando a paso continuo. La mejora constante en el procesamiento hace que ataques criptográficos de cálculo informático sean más realistas. Nuevos algoritmos criptográficos y técnicas de generación de clave pública son desarrollados a paso continuo. Nuevos servicios de seguridad y mecanismos de seguridad son desarrollados a paso acelerado. Un método constante para elegir servicios de seguridad y mecanismos de seguridad y para intercambiar atributos requeridos por los mecanismos es importante para la seguridad de la compleja estructura de Internet. Sin embargo, un sistema que se sierra en si mismo en un único algoritmo criptográfico, técnica de intercambio de claves o mecanismos de seguridad se convertirán cada vez más vulnerable a medida que pasa el tiempo.

UDP es un Protocolo de datagrama no confiable y por lo tanto su uso en ISAKMP introduce un número de consideraciones de seguridad. Ya que UDP no es confiable, pero un protocolo de administración de claves debe ser confiable, la confiabilidad se construye dentro de ISAKMP. Mientras que ISAKMP utiliza UDP como su mecanismo de trasporte, no confía en la información de UDP (por ejemplo la suma de comprobación o longitud) para su procesamiento.

Otro tema que debe ser considerado en el desarrollo de ISAKMP es el efecto de firewalls en el protocolo. Muchos de los firewalls filtran los paquetes UDP salientes asiendo que la dependencia en UDP sea cuestionable en ciertos entornos.

Un número de consideraciones de seguridad muy importantes están presentadas en [SERC-ARCH]. Uno soporta repetición [One bears repeating]. Una vez que la clave de sesión privada es creada, debe ser almacenada en forma segura. No proteger adecuadamente las claves privadas para accesos internos o externos al sistema anula totalmente cualquier protección proporcionada por los servicios de seguridad IP.

Consideraciones de IANA

Este documento contiene muchos números "mágicos" que serán mantenidos por la IANA. Esta sección explica el criterio que será usado por la IANA para asignar números adicionales en cada una de estas listas.

Dominio de Interpretación

El Dominio de Interpretación (DOI) es un campo de 32-bits que identifica el dominio bajo el cual la negociación de la SA se esta llevando a cabo. Los pedidos de asignaciones de nuevos DOI deben

estar acompañados de un RFC para el tráfico estándar el cual describe el dominio específico.

Protocolos de Seguridad Soportados

ISAKMP está diseñado para proporcionar gestión de claves y negociación de SA para varios protocolos de seguridad. Los pedidos de identificadores para protocolos de seguridad adicionales deben estar acompañados de un RFC para el tráfico estándar que describe el protocolo de seguridad y su relación con ISAKMP.

Agradecimientos

Dan Harkins, Dave Carrel, and Derrell Piper of Cisco Systems proporcionaron asistencia de diseño para el protocolo y coordinación para los documentos [IKE] [IPDOI].

Hilarie Orman, a través del protocolo de intercambio Oakley, a tenido influencia significativa en el diseño de ISAKMP

Marsha Gross, Bill Kutz, Mike Oehler, Pete Sell, and Ruth Taylor proporcionaron información para este documento.

Scott Carlson colaboró con el prototipo TIS DNSSEC FreeBSD para el uso con el prototipo de ISAKMP.

Jeff Turner y Steve Smalley contribuyeron al desarrollo del prototipo e integración con ESP y AH.

Mike Oehler y Pete Sell realizaron pruebas de interoperatibilidad con otras implementaciones de ISAKMP.

Thanks to Carl Muckenhirn de SPARTA, Inc. por su asistencia con LaTeX.

Referencias

[ANSI] ANSI, X9.42: Public Key Cryptography for the Financial Services Industry -- Establishment of Symmetric Algorithm Keys Using Diffie-Hellman, Working Draft, April 19, 1996.

[BC] Ballardie, A., and J. Crowcroft, Multicast-specific Security Threats and Countermeasures, Proceedings of 1995 ISOC Symposium on Networks & Distributed Systems Security, pp. 17-30, Internet Society, San Diego, CA, February 1995.

[Berge] Berge, N., "UNINETT PCA Policy Statements", RFC 1875, December 1995.

[CW87] Clark, D.D. and D.R. Wilson, A Comparison of Commercial and Military Computer Security Policies, Proceedings of the IEEE Symposium on Security & Privacy, Oakland, CA, 1987, pp. 184-193.

[DNSSEC] D. Eastlake III, Domain Name System Protocol Security Extensions, Work in Progress.

[DOW92] Diffie, W., M.Wiener, P. Van Oorschot, Authentication and Authenticated Key Exchanges, Designs, Codes, and Cryptography, 2, 107-125, Kluwer Academic Publishers, 1992.

[IAB] Bellovin, S., "Report of the IAB Security Architecture Workshop", RFC 2316, April 1998.

[IKE] Harkins, D., and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[IPDOI] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[Karn] Karn, P., and B. Simpson, Photuris: Session Key Management Protocol, Work in Progress.

[Kent94] Steve Kent, IPSEC SMIB, e-mail to ipsec@ans.net, August 10, 1994.

[Oakley] Orman, H., "The Oakley Key Determination Protocol", RFC 2412, November 1998.

[RFC-1422] Kent, S., "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management", RFC 1422, February 1993.

[RFC-1949] Ballardie, A., "Scalable Multicast Key Distribution", RFC 1949, May 1996.

[RFC-2093] Harney, H., and C. Muckenhirn, "Group Key Management Protocol (GKMP) Specification", RFC 2093, July 1997.

[RFC-2094] Harney, H., and C. Muckenhirn, "Group Key Management Protocol (GKMP) Architecture", RFC 2094, July 1997.

[RFC-2119] Bradner, S., "Key Words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[Schneier] Bruce Schneier, Applied Cryptography - Protocols, Algorithms, and Source Code in C (Second Edition), John Wiley & Sons, Inc., 1996.

[SEC-ARCH] Atkinson, R., and S. Kent, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[STD-2] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1700, October 1994. See also: http://www.iana.org/numbers.html

Direcciones de los Autores

Douglas Maughan
National Security Agency
ATTN: R23
9800 Savage Road
Ft. Meade, MD. 20755-6000

Phone: 301-688-0847
EMail:wdm@tycho.ncsc.mil

Mark Schneider
National Security Agency
ATTN: R23
9800 Savage Road
Ft. Meade, MD. 20755-6000

Phone: 301-688-0851
EMail:mss@tycho.ncsc.mil

Mark Schertler
Securify, Inc.
2415-B Charleston Road
Mountain View, CA 94043

Phone: 650-934-9303
EMail:mjs@securify.com

Jeff Turner
RABA Technologies, Inc.
10500 Little Patuxent Parkway
Columbia, MD. 21044

Phone: 410-715-9399
EMail:jeff.turner@raba.com

Declaración de Copyright Completa

Notas del Traductor

Las Siguientes palabras no han sido traducidas y su significado es el siguiente:

- Nonce: Aliatoriamente, cadena de texto única que es encriptada con datos y que luego es usada para detectar ataques contra el sistema que envía el dato encriptado. Un NONCE es usado específicamente para la autentificación y para asegurar que el dato encriptado es diferente cada vez que es encriptado. (Definición extraída del Diccionario de IBM Corp.)

- Perfect Forward Secrecy: En criptografía, en un protocolo de establecimiento de clave, la condición en la cual el acuerdo de una clave de sesión o clave privada de largo plazo posterior a una determinada sesión no comprometa ninguna (clave) sesión anterior.(Definición extraída de: www.its.bldrdoc.gov.)

- Bootstrapping: proceso por el cual una referencia inicial del servicio de nombramiento es obtenida.

Los Términos que aparecen entre "[]" que no sean referencias reflejan la palabra/s en inglés de las palabra/s que se encuentran (en español) a la izquierda, debido a que NO ESTOY SEGURO de que sea la correcta traducción del término o simplemente para que no se pierda el VERDADERO sentido del texto.

Esta presente traducción fue realizada por Hugo Adrian Francisconi para mi tarjado de tesis de "Ingeniero en Electrónico" en la Facultad U.T.N. (Universidad Nacional Tecnología) Regional Mendoza - Argentina. Si le interesa IPsec y quieres saber más podes bajarte mi trabajo de tesis, "IPsec en Ambientes IPv4 e IPv6" de http://codarec6.frm.utn.edu.ar, para el cual traduje varios RFCs al español relacionados con IPsec. Cualquier sugerencia debate o comentario sobre este presente tema o traducción será bien recibida en adrianfrancisconi@yahoo.com.ar

Se a realizado el máximo esfuerzo para hacer de esta traducción sea tan completa y precisa como sea posible, pero no se ofrece ninguna garantía implícita de adecuación a un fin en particular. La información se suministra "tal como está". El traductor no será responsable ante cualquier persona o entidad con respecto a cualquier pérdida o daño que pudiera resultar emergente de la información contenida en está traducción.

Datos del Traductor

Nombre y Apellido del Traductor: Hugo Adrian Francisconi
Domicilio: Carril Godoy Cruz 2801, Villa Nueva-Guay Mallen-Mendoza-Argentina
Código Postal: 5500
Tel: 054-0261-4455427
E-mail: adrianfrancisconi@yahoo.com.ar