3.3 IKE (INTERNET KEY EXCHANGE)

The key management portion of IPSec involves the determination and distribution of secret keys.

The IPSec support two types of key management:

Manual: A system administrator manually configures each system with its own keys and with the keys of other communicating systems.

Automated: This system supports on-demand creation of keys for SAs and supports use of large system. The automated key management protocol for IPsec is called ISAKMP/Oakly.

ISAKMP

ISAKMP defines procedures and formats to establish, negotiate, modify, and delete security associations. ISAKMP defines payload for exchanging key generation and authentication data.

Initiator Cookie (64 bits): Cookie of entity that initiated SA establishment, SA notification, or SA deletion.

Responder Cookie (64 bits): Cookie of responding entity; null in first message from initiator.

Next Payload (8 bits): Indicates the type of the first payload in the message.

Major Version (4 bits): Indicates major version of ISAKMP in use.

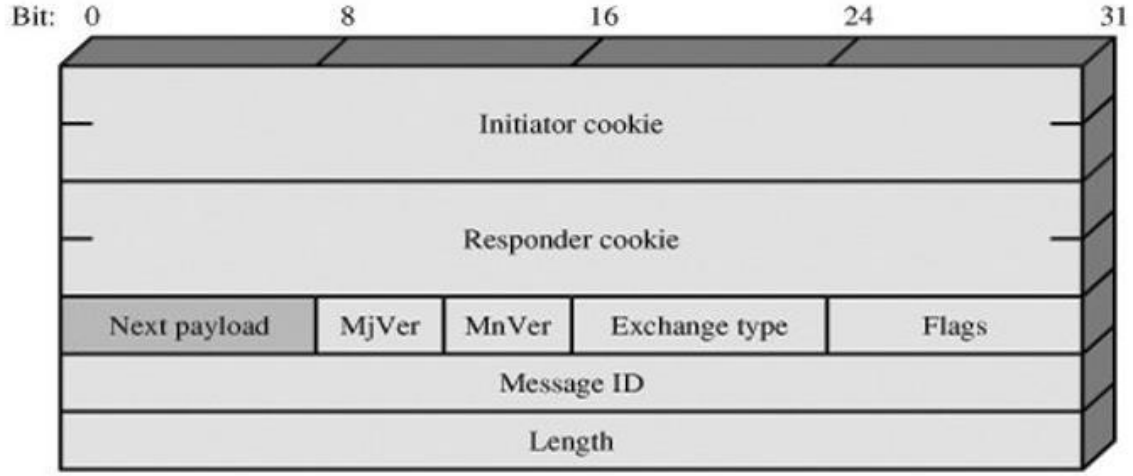
Minor Version (4 bits): Indicates minor version in use.

Exchange Type (8 bits): Indicates the type of exchange.

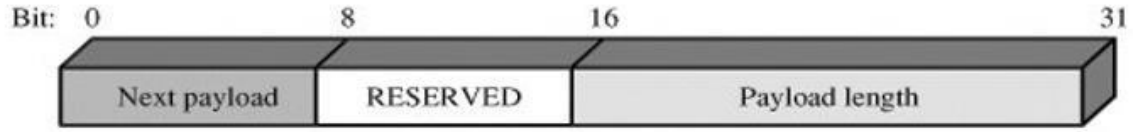
Flags (8 bits): Indicates specific options set for this ISAKMP exchange.

Message ID (32 bits): Unique ID for this message.

Length (32 bits): Length of total message (header plus all payloads) in octets.



(a) ISAKMP header



(b) Generic payload header

ISAKMP Payload Types

Type	Description
Security Association (SA)	Used to negotiate security attributes and indicate the DOI and
Proposal (P)	Used during SA negotiation; indicates protocol to be used and number
Transform (T)	Used during SA negotiation; indicates transform and related SA
Key Exchange (KE)	Supports a variety of key exchange techniques.
Identification (ID)	Used to exchange identification information
Certificate (CERT)	Used to transport certificates and other certificate- related
Certificate Request (CR)	Used to request certificates; indicates the types of certificates
Hash (HASH)	Contains data generated by a hash function.
Signature (SIG)	Contains data generated by a digital signature function.
Nonce (NONCE)	Contains a nonce.
Notification (N)	Used to transmit notification data, such as an error condition.
Delete (D)	Indicates an SA that is no longer valid.

ISAKMP messages

Responder-Lifetime: Communicates the SA lifetime chosen by the responder.

Replay-Status: Used for positive confirmation of the responder's election of whether

or not the responder will perform anti-replay detection.

Initial-Contact: Informs the other side that this is the first SA being established with the remote system.

The Delete payload: Indicates that the sender has deleted the SA from its database.

ISAKMP Exchanges

The Base Exchange: Allows key exchange and authentication to be transmitted together.

The Identity Protection Exchange: Expands the base to protect the users' identities.

The Authentication Only Exchange: Used to perform mutual authentication, without a key exchange.

The Aggressive Exchange: Provides identity protection.

The Informational Exchange: Used for one-way transmittal of information for SA management.

Features of IKE Key Determination

Algorithm is characterized by five important features:

1. It employs a mechanism known as cookies to thwart clogging attacks
2. It enables the two parties to negotiate a group; this, in essence, specifies the global parameters of the Diffie-Hellman key exchange
3. It uses nonces to ensure against replay attacks
4. It enables the exchange of Diffie-Hellman public key values
5. It authenticates the Diffie-Hellman exchange to thwart man-in-the-middle attacks

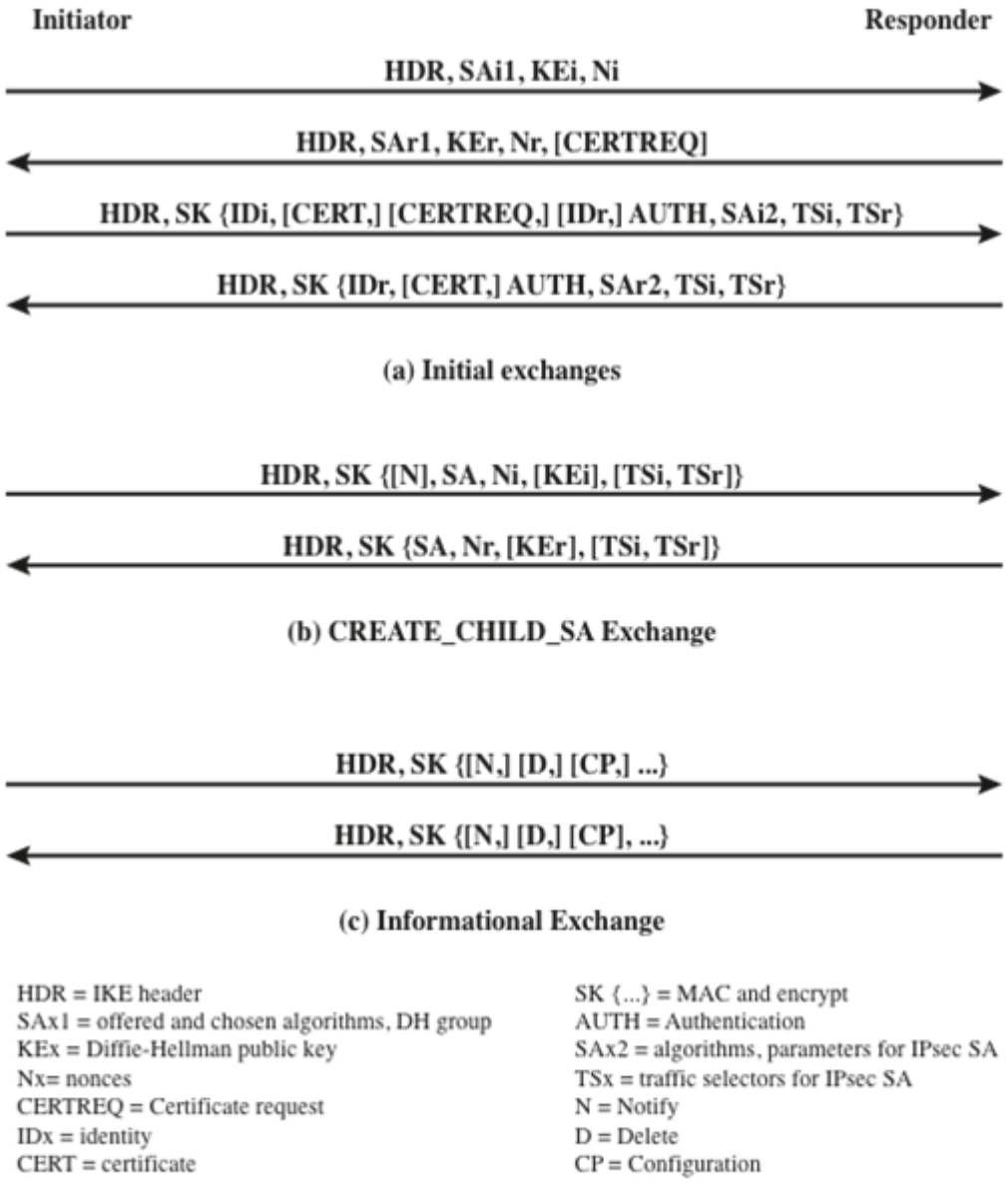


Figure IKEv2 Exchanges

The IKEv2 protocol involves the exchange of messages in pairs. The first two pairs of exchanges are referred to as the initial exchanges. In the first exchange, the two peers exchange information concerning cryptographic algorithms and other security parameters they are willing to use along with nonces and Diffie-Hellman (DH) values. The result of this exchange is to set up a special SA called the IKE SA (see Figure 9.2). This SA defines parameters for a secure channel between the peers over which subsequent message exchanges take place. Thus, all subsequent IKE message

exchanges are protected by encryption and message authentication. In the second exchange, the two parties authenticate one another and set up a first IPsec SA to be placed in the SADB and used for protecting ordinary (i.e. non-IKE) communications between the peers. Thus, four messages are needed to establish the first SA for general use.

The CREATE_CHILD_SA exchange can be used to establish further SAs for protecting traffic. The informational exchange is used to exchange management information, IKEv2 error messages, and other notifications.

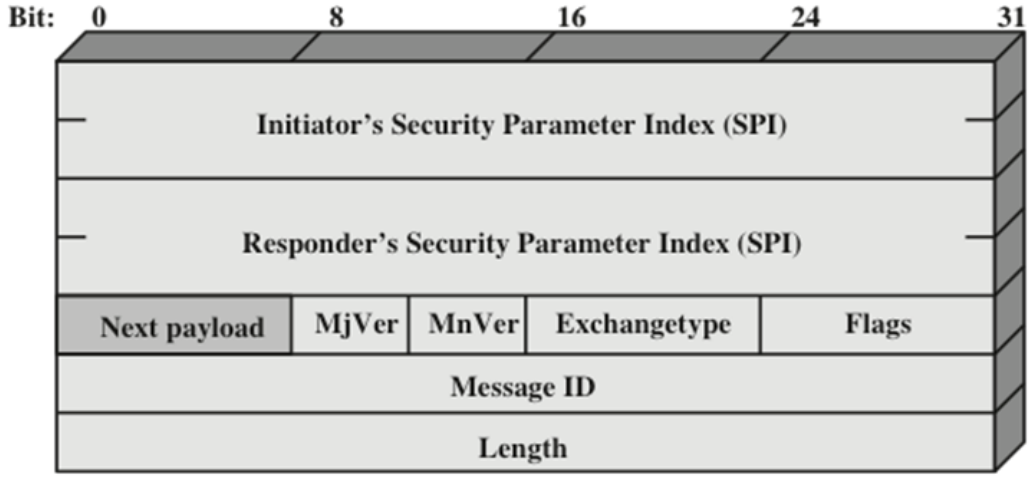


Figure IKE Formats