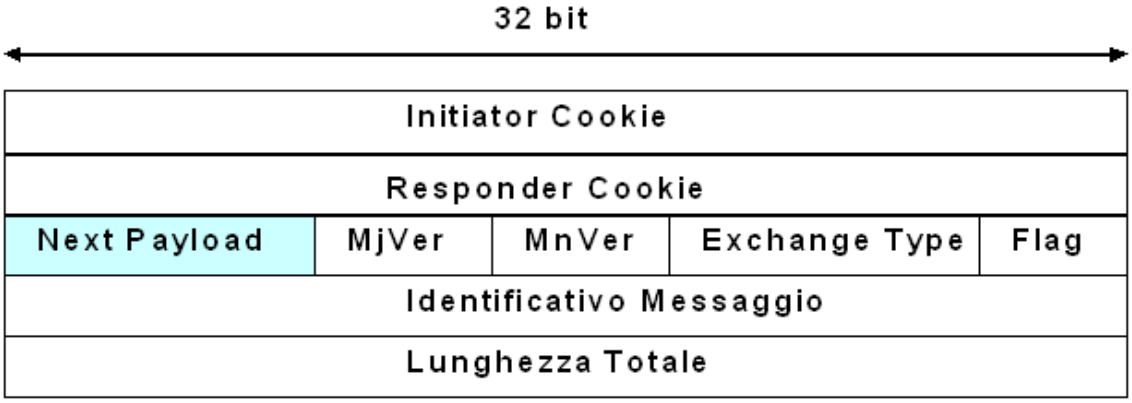
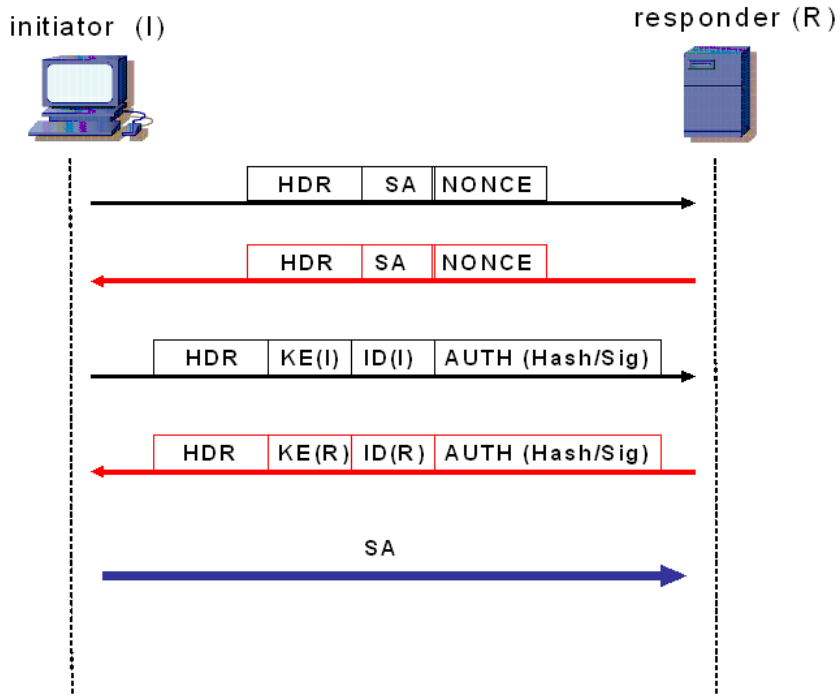
ISAKMP Internet Security and Key Management Protocol:



- **Initiator Cookie (64bit):** contiene un numero pseudocasuale inserito dall'entità che avvia la negoziazione di una nuova SA; tale valore sarà applicato come ingresso alle funzioni di digest utilizzate per calcolare le componenti crittografiche all'autenticazione
- **Responder Cookie (64bit):** contiene un numero pseudocasuale inserito dall'entità che risponde alla negoziazione di una nuova SA; tale valore sarà applicato come ingresso alle funzioni di digest esattamente come prima indicato
- **Next Payload (8bit):** indica il tipo di carico utile ISAKMP che segue l'intestazione generale
- **Major Version (4 bit):** indica la versione del protocollo ISAKMP in uso
- **Minor Version (4 bit):** indica la versione del protocollo ISAKMP in uso
- **Exchange Type (8bit):** indica il modello di interazione a cui si riferisce il messaggio ISAKMP
- **Flag (8 bit):** permette di comunicare una serie di informazioni specifiche relative al messaggio ISAKMP (ad es. il bit **Encryption**)
- **Identificativo Messaggio (32 bit):** identificativo univoco del messaggio ISAKMP
- **Lunghezza Totale (32 bit):** dimensione totale del messaggio (header più successivi payload).

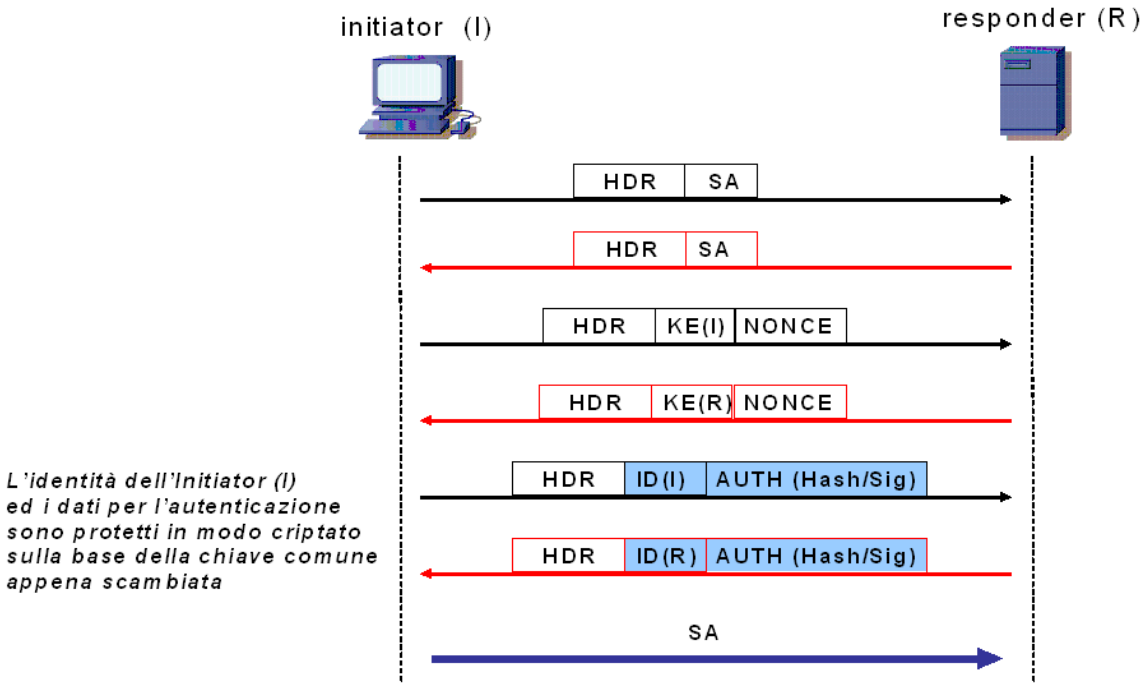
Type	Valore	Funzione
Security Association (SA)	1	natura delle SA che si sta negoziando
Proposal (P)	2	natura dei meccanismi di sicurezza per la SA
Transform (T)	3	dettagli sui meccanismi di sicurezza per la SA
Key Exchange (KE)	4	permette di scambiare chiavi e sistemi crittografici
Identification (ID)	5	informazioni per identificare le entità
Hash (HASH)	8	informazioni per stabilire integrità dati (funzioni digest)
Segnature (SIG)	9	informazioni per stabilire integrità dati e non ripudio (funzioni di segnatura digitale)
Nonce (NONCE)	10	permette di scambiare un numero pseudocasuale

Base Exchange per una nuova SA:



La SA creata è un'associazione unilaterale che consente ad (I) di usufruire di uno dei servizi offerti da IPSEC, per ogni datagramma IP trasmesso ad (R); se anche l'altra entità IP vuole usufruire di un servizio di autenticazione o codifica, occorre attivare una seconda SA, ripetendo lo scambio sopra indicato.

Identity Protection Exchange per una nuova SA:



Aggressive Exchange per una nuova SA: