ISAKMP IKE internet Key Exchange

Il protocollo ISAKMP definisce la struttura di messaggi ed una serie di modelli di interazione per conseguire la negoziazione di una nuova SA tra due entità IP; di tutti gli schemi compatibili con ISAKMP quello che ha avuto maggiore successo è l'**IKE** (**Internet Key Exchange**).

Per la negoziazione di un canale sicuro tra le due entità sono disponibili due modi:

Phase 1 Mode:

- **Main Mode:** rappresenta una implementazione ISAKMP Identity Protection Exchange
- **Aggressive Mode:** rappresenta una implementazione ISAKMP Aggressive Exchange

Se tra due entità IP esiste già una SA attiva, IKE definisce anche un terzo modo:

- **Quick Mode:** per ottenere uno scambio di materiale criptato e la negoziazione dei parametri relativi alle nuove SA associate ai singoli canali sicuri IPSEC; un'associazione Phase 1 può essere utilizzata per la negoziazione di molteplici **SA di tipo Phase 2**.

IKE prevede tre possibilità di autenticare il materiale crittografico, i cookie (numeri pseudocasuali) ed i nonce (permette lo scambio di numeri pseudocasuali) scambiati tra le due entità IP:

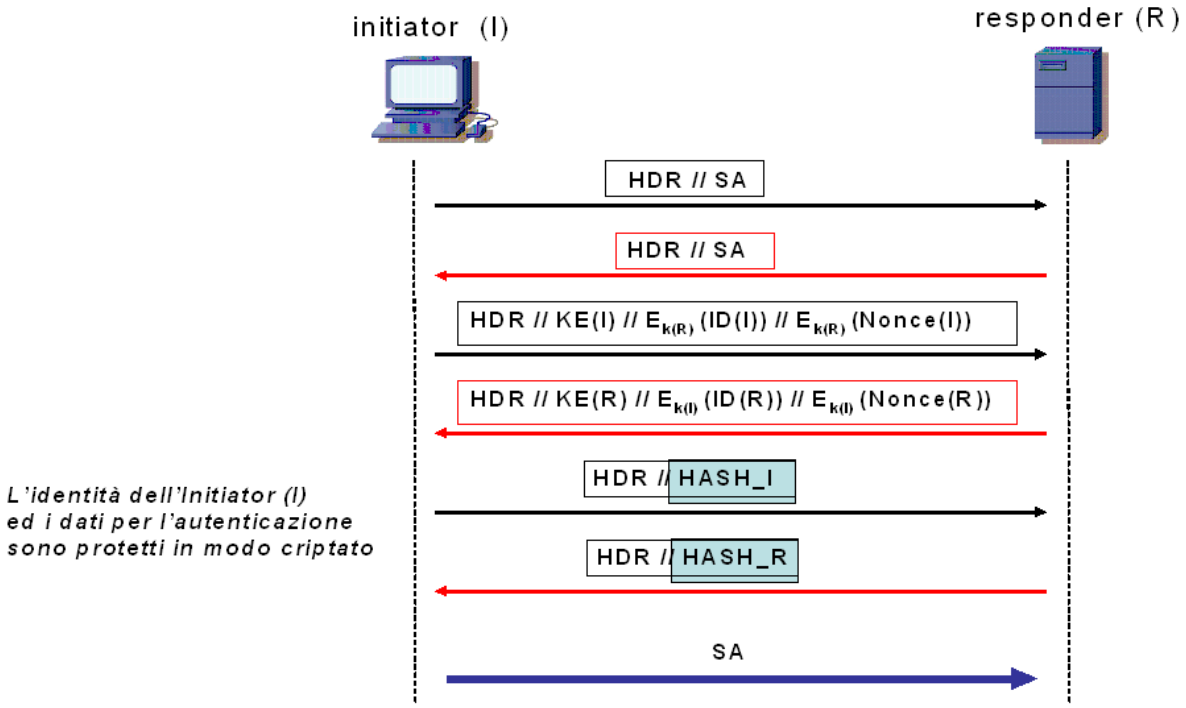
- **schema a chiave pubblica e privata**
- **schema a chiave comune inizialmente condivisa** (**preshared-key**)
- **segnatura digitale**

L'autenticazione tramite chiave pubblica richiede all'entità coinvolte il calcolo e la verifica delle seguenti componenti:

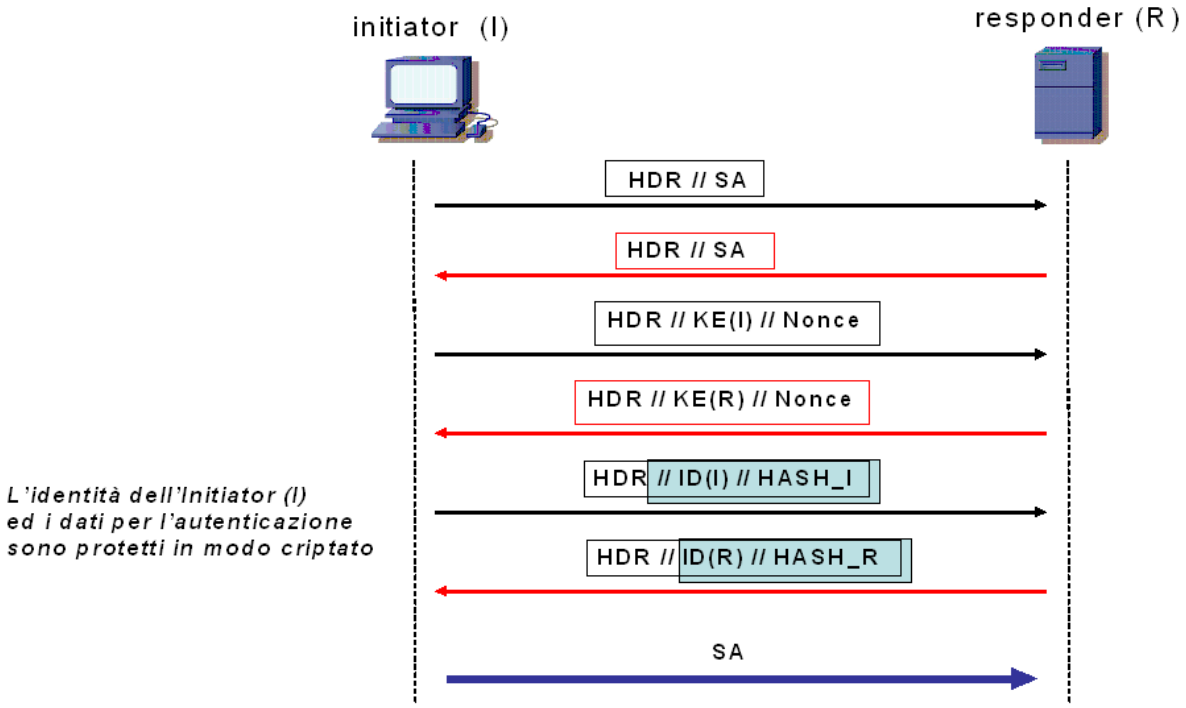
- **K1 = H (Nonce (I) // Nonce (R))**
- **S = HMAC (K1, Cookie (I) // Cookie (R))**
- **HASH_I = HMAC (S, g^{xi} // g^{xr} // Cookie (I) // Cookie (R) // SA // ID (I))**
- **HASH_R = HMAC (S, g^{xr} // g^{xi} // Cookie (R) // Cookie (I) // SA // ID (R))**

g^{xi} = chiave pubblica di (I)
g^{xr} = chiave pubblica di (R)

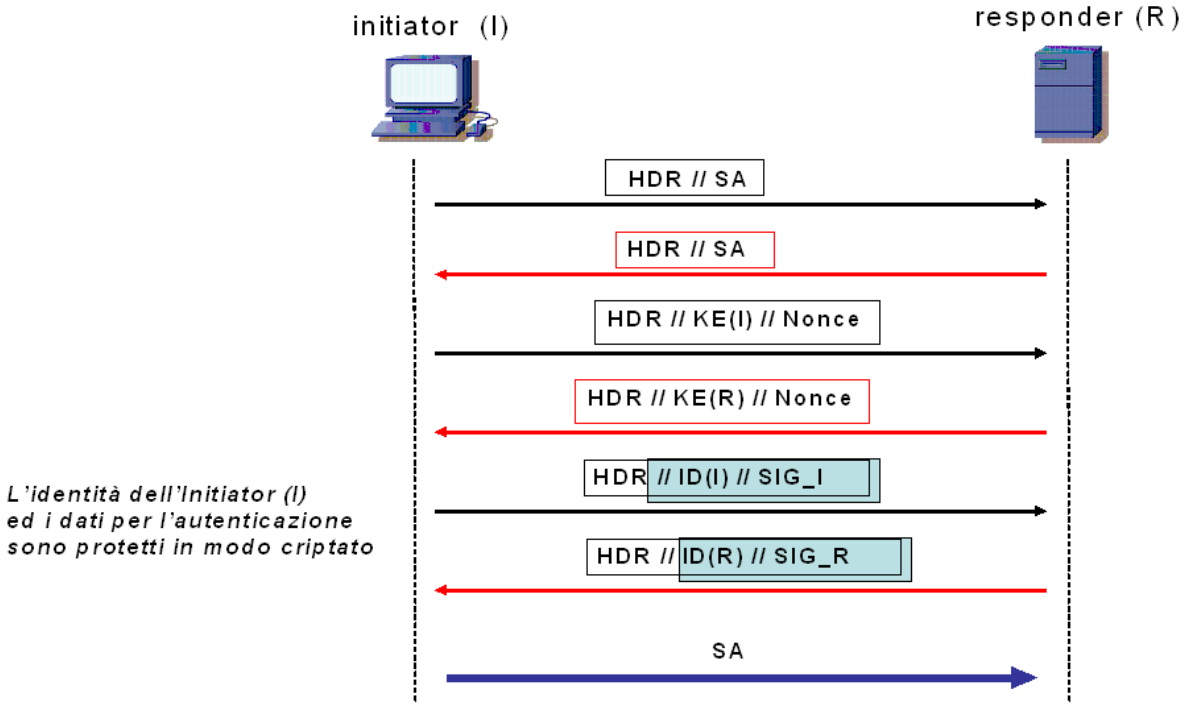
Phase 1 Main Mode (chiave pubblica):



Phase 1 Main Mode (Pre-Shared Key):



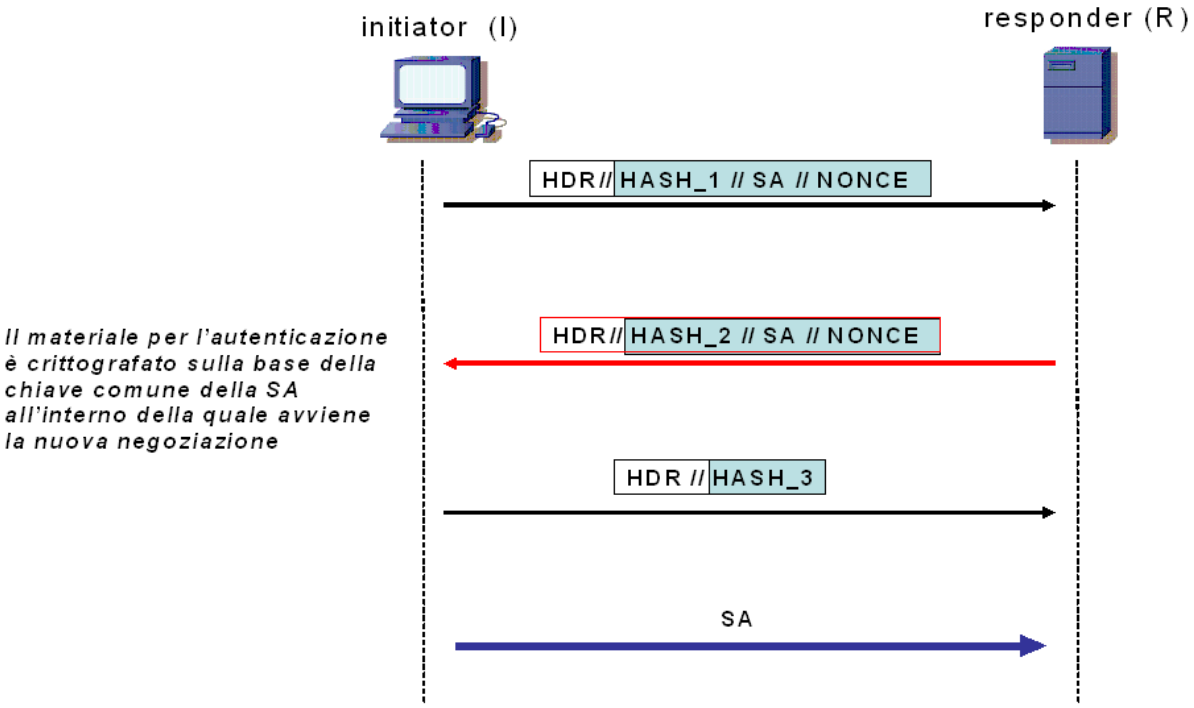
Phase 1 Main Mode (signature digitale):



Phase 1 : configurazione IKE (cisco system)

cripto isakmp policy 1
encryption 3des (des, aes)
hash md5 (HMAC version)
group2 (diffie-helmann)
lifetime (seconds or kilobytes)
authentication pre-shared
show cry isakmp policy

Phase 2 (Quik Mode):



Nell'eventualità che non sia richiesta la computazione di una nuova chiave comune, in accordo allo schema Diffide-Hellman, alle entità coinvolte alla negoziazione della SA, è richiesto il calcolo e la verifica delle seguenti componenti crittografiche:

- **S_{k_d} = HMAC (S, g^{xy} // Cookie (I) // Cookie (R) // 0)**
- **S_{k_a} = HMAC (S, S_{k_d} // g^{xy} // Cookie (I) // Cookie (R) // 1)**
- **HASH_1 = HMAC (S_{k_a}, M-ID // SA //Nonce (I))**
- **HASH_2 = HMAC (S_{k_a}, M-ID // Nonce (I) // SA // Nonce (R))**
- **HASH_3 = HMAC (S_{k_a}, 0 // M-ID // Nonce (I) // Nonce (R))**

Il calcolo di **S** dipende dalla procedura utilizzata per l'autenticazione

M-ID rappresenta il valore trasportato nel campo **identificativo messaggio** all'interno dell'intestazione ISAKMP.