Lo standard IPSec non prevede una fase di negoziazione in cui uno dei *peer* assegni dinamicamente all'altro parametri di rete come indirizzo IP e server DNS, come invece avviene di norma nelle situazioni tipiche dell'accesso remoto. L'impiego combinato di IPSec e di L2TP consente di risolvere questa limitazione.

Per primo viene stabilito un normale tunnel IPSec tra l'utente ed il concentratore VPN.
Durante la fase IKE avviene un'autenticazione del canale: i due peer si identificano l'un l'altro per mezzo di certificati digitali emessi da "Certification Authority"

Sul canale sicuro cosi costituito avviene un nuovo dialogo tra client e concentratore VPN seguendo questa volta il protocollo L2TP ed in questa seconda fase viene effettuata una nuova autenticazione allo scopo di riconoscere l'utente attraverso il meccanismo di PAP e CHAP (username e password) ovvero con EAP (certificati X.509, Token Card, One-Time Password).

Una volta che l'utente è stato riconosciuto, la fase L2TP si conclude con l'assegnazione al client dell'indirizzo IP sulla rete remota e dei restanti parametri di rete.