L2TP e PPTP definiscono i meccanismi di instaurazione, abbattimento e controllo dei tunnel, ma non le procedure di autenticazione che permettono al concentratore VPN di accertare l'identità del client.

A questo scopo si appoggiano ai protocolli standard normalmente impiegati negli scenari di accesso remoto, dei quali segue una breve descrizione:

- **Password Authentication Protocol (PAP):** è un semplice protocollo che prevede l'autenticazione con "username e password", entrambi trasmessi in chiaro sul canale. Per questo motivo è assolutamente inadatto a scenari VPN a meno che il canale non sia già sicuro al momento dell'invio della password, come nel caso di L2TP/IPSec.

- **Challenge Handshake Authentication Protocol (CHAP):** versione migliorata del protocollo PAP; prevede l'impiego di "username e password" ma evita il passaggio di quest'ultima in chiaro sul canale grazie all'uso di *"challenge"*.

- **Microsoft Challenge Handshake Authentication Protocol (MS-CHAP):** è un'estensione di CHAP, sviluppata da Microsoft e successivamente standardizzata in seno all'IETF. Consente tra l'altro di negoziare l'impiego del protocollo MPPE per la crittografia dei dati trasferiti durante la sessione punto-punto, permettendo quindi la realizzazione di VPN mediante regole sicure senza ricorrere ad IPSec. E' disponibile in due versioni di cui la prima è supportata a partire da Windows 95 e la seconda a partire da Windows 98.

- **Extensible Authentication Protocol (EAP):** rappresenta una risposta alle esigenze di metodi di autenticazione più sicuri ed al passo con i tempi negli scenari di accesso remoto. Consente inoltre l'utilizzo di certificati digitali, token card e one-time password. E' supportato in modo nativo da Windows 2000 e Windows XP.