SECONDA PARTE Quesito 4

Per ottenere un servizio pubblico di scambio dati privati (cioè dati e informazioni appartenenti ad una organizzazione, società, istituzione, azienda, ...) la soluzione ideale risulta rendere l'Intranet privata (ovvero tutti i servizi aziendali) accessibile da remoto, per esempio tramite **VPN**.
L'accesso alla rete aziendale tramite VPN consente a un utente aziendale 'mobile' di operare sui servizi interni come se fosse connesso in locale.

In questo caso diventa cruciale la questione della sicurezza, dato che informazioni nativamente private (della Intranet locale) devono per forza di cose circolare su rete pubblica.
VPN affronta questo problema tramite il protocollo tunnel **IPSec**.
IPSec garantisce:

1. **Autenticazione simmetrica** (dei client VPN e del server VPN aziendale) tramite lo scambio di chiavi di Diffie-Helmann (sottoprotocollo **IKE**).
2. **Integrità e segretezza** tramite sottoprotocollo **ESP**.

Da notare che IPSec non necessità di autenticazione tramite Certificato Digitale perché il servizio non è pubblico (ma riservato agli utenti della VPN dotati di account privati).

Testi di:

prof. Paolo Ollari
prof. Francesc'Antonio Franco
prof. Alberto Paganuzzi

ITIS "L. Da Vinci", Parma