L'infrastruttura **PKI (Public Key Infrastructure)** è un insieme di apparati, software, policy e procedure in grado di creare, gestire, archiviare, distribuire e revocare certificati digitali.

L'infrastruttura rende possibile la certificazione dell'identità di un "end-user" da parte di una Certification Authority (CA) per mezzo di un certificato digitale.

Il possesso di registrazione presso la CA prevede che l'utente generi una richiesta di certificato e la inoltri alla CA in formato "PKCS#10".

La CA successivamente effettua le seguenti operazioni:

- Verifica le credenziali del richiedente
- Trasforma la richiesta in un certificato digitale in formato X.509
- Firma il certificato con la sua chiave privata
- Invia il certificato al richiedente.

Il certificato X.509 contiene una serie di informazioni di identificazione, la chiave pubblica dell'utente nonché l'intervallo di validità del certificato stesso.
La firma della CA certifica l'utente associando le informazioni di identità alla chiave pubblica dello stesso.

I certificati digitali possono essere impiegati per l'autenticazione dei *peer* nella fase preliminare all'instaurazione di un tunnel IPSec, implementata tramite IKE (Internet Key Exchange).

Quando un utente remoto richiede al VPN Concentrator l'instaurazione del tunnel IPSec, esso provvede a :

- Ricezione del certificato digitale del peer
- Verifica dell'autenticità del certificato mediante la chiave pubblica della CA che lo ha emesso (il peer deve possedere il certificato della CA contenente la relativa chiave pubblica)
- Controllo della scadenza del certificato
- Verifica presso la CRL (Certficate Revocation List) che il certificato non sia stato revocato; i certificati X.509 contengono per questo scopo al loro interno un puntatore ai CRL Distribution Point da consultare.