IPSEC

Il progetto di inserire sistemi crittografici direttamente a livello IP è stato esteso per applicazioni sia IPv4 che IPv6.

L'architettura **IPSEC** permette di ottenere una maggiore protezione sui dati trasmessi introducendo le funzionalità necessarie, affinché le entità IP coinvolte possano:

- selezionare funzioni crittografiche
- determinare gli algoritmi per ciascun servizio
- scambiarsi le chiavi relative.

L'architettura IPSEC si compone di due protocolli:

- **Authentication Protocol (AH):** responsabile del servizio di autenticazione
- **Encapsulation Security Payload Protocol (ESP):** responsabile della riservatezza dei dati.