Internet Key Exchange protokol, je protokol, ki omogoča izmenjavo občutljivih podatkov oz. ključev za komunikacijo, preko interneta. Razne verzije so definirane v RFC 2409, RFC 4306, RFC 5282.

IKE deluje v dveh fazah in vsaka faza ima nekaj načinov delovanja, kjer se izmenjujeta hitrost komunikacije oz. opravila izmenjave in varnost. IKE uporablja PKI ali PSK (pre-shared key) za avtentikacijo odjemalcev med seboj.

1.Faza

- Vzpostavitev dvosmernega IKE SA-ja (INIT in AUTH), ta je **strogo ločen od IPsec SA-ja** in se uporablja samo za izmenjavo ključev (imenuje se tudi ISAKMP SA)
- V IKE SA se vzpostavi ključ za varovanje nadaljne komunikacije glede izmenjave ključev (Avtentikacija se izvede s PSK, PKI ali podpisom)
- V tej fazi sta dva načina delovanja *Aggressive mode (krajši, vendar razkrije identiteto odjemalcev)* in *Main mode (daljši, skrije identiteto)*

2.Faza

- IKE generira ključe za druge storitve, kot je npr. IPsec, tako se ustvari IPsec SA (CREATE_CHILD in INFO)
- Edini način je *Quick Mode*