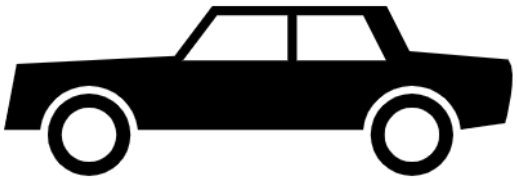
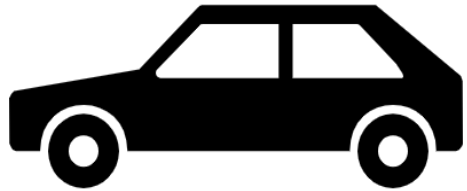
$$Cert_R||E_{pk_S}(key_r + SN_S)||E_{pk_S}(E_{sk_R}(H(key_r + SN_S)))$$

S



R



I can recover $(key_r + SN_S)$ with my sk_S and $H(key_r + SN_S)$ with my sk_S and your pk_R.
Let me check those hashes match before we start communicating...