Client

Co zná:
- Pc - veřejný klíč klienta
- Sc - soukromý klíč klienta
- Ps - veřejný klíč serveru

+ Rc - nový náhodně vygenerovaný AES-256 klíč

Server

Co zná:
- Ps - veřejný klíč serveru
- Ss - soukromý klíč serveru
- Pc - veřejný klíč klienta

+ Rs - nový náhodně vygenerovaný AES-256 klíč

1. $e_{Ps}(Rc) \mid e_{Rc}(pseudo) \mid MAC_{Rc}(e_{Rc}(pseudo))$ →

   $d_{Ss}(e_{Ps}(Rc)) \Rightarrow Rc$
   $d_{Rc}(e_{Rc}(pseudo)) \Rightarrow pseudo$

2. ← $e_{Pc}(Rs) \mid e_{Rs}(Rc) \mid MAC_{Rs}(e_{Rs}(Rc))$

   $d_{Sc}(e_{Pc}(Rs)) \Rightarrow Rs$
   $d_{Rs}(e_{Rs}(Rc)) \Rightarrow Rc' \quad =?= \quad Rc_{původní}$

   autentizace serveru

3. K:=sha(Rc | Rs) - výpočet nového sdíleného klíče pro AES-256

   K:=sha(Rc | Rs) - výpočet nového sdíleného klíče pro AES-256

   $e_K(Rs) \mid MAC_K(e_K(Rs))$ →

   $d_K(e_K(Rs)) \Rightarrow Rs' \quad =?= Rs_{původní}$

   autentizace klienta