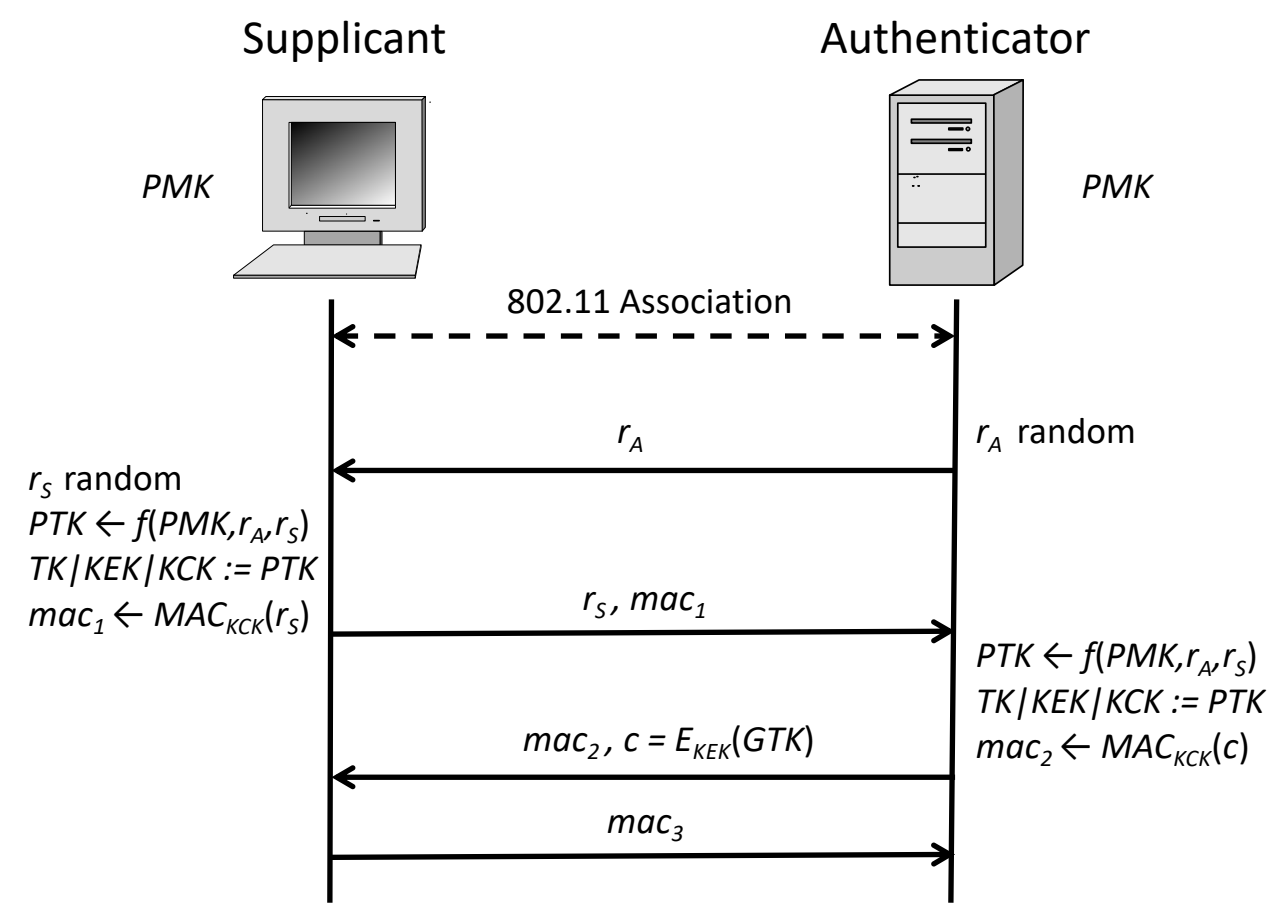
Supplicant
Authenticator
PMK
PMK
802.11 Association
r_A
r_A random
r_S random
$PTK \leftarrow f(PMK,r_A,r_S)$
$TK|KEK|KCK := PTK$
$mac_1 \leftarrow MAC_{KCK}(r_S)$
r_S, mac_1
$PTK \leftarrow f(PMK,r_A,r_S)$
$TK|KEK|KCK := PTK$
$mac_2 \leftarrow MAC_{KCK}(c)$
mac_2, $c = E_{KEK}(GTK)$
mac_3