

Kerberos Version 5: message exchanges

To obtain ticket-granting ticket

$C \rightarrow AS:$ Options, ID_C , $Realm_C$, ID_{TGS} ,
Times, $Nonce_1$

$AS \rightarrow C:$ $Realm_C$, ID_C , $Ticket_{TGS}$, $Info_{TGS}$

$Ticket_{TGS} =$
 $E_{K_{TGS}}[Flags, K_{C,TGS}, Realm_C, ID_C, AD_C, Times]$

$Info_{TGS} =$
 $E_{K_C}[K_{C,TGS}, Times, Nonce_1, Realm_{TGS}, ID_{TGS}]$

To obtain service-granting ticket

$C \rightarrow TGS:$ Options, ID_V , Times, Nonce₂,
 $Ticket_{TGS}$, $Authenticator_C$

$TGS \rightarrow C:$ Realm_C, ID_C , $Ticket_V$, $Info_V$

$Ticket_{TGS} =$

$E_{K_{TGS}}[\text{Flags}, K_{C,TGS}, \text{Realm}_C, ID_C, AD_C, \text{Times}]$

$Ticket_V =$

$E_{K_V}[\text{Flags}, K_{C,V}, \text{Realm}_C, ID_C, AD_C, \text{Times}]$

$Authenticator_C = E_{K_{C,TGS}}[ID_C, \text{Realm}_C, TS_1]$

$Info_V = E_{K_{C,TGS}}[K_{C,V}, \text{Times}, \text{Nonce}_2, \text{Realm}_V, ID_V]$

To obtain service from V

$C \rightarrow V$: Options, ID_V , $Ticket_V$, $Authenticator_V$

$V \rightarrow C$: $E_{K_{C,V}}[TS_2, Subkey, Seq\#]$

$Ticket_V =$

$E_{K_V}[Flags, K_{C,V}, Realm_C, ID_C, AD_C, Times]$

$Authenticator_V =$

$E_{K_{C,V}}[ID_C, Realm_C, TS_2, Subkey, Seq\#]$