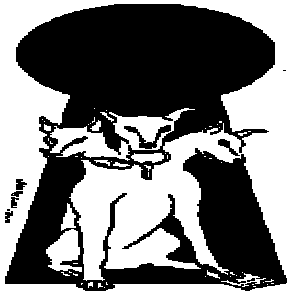
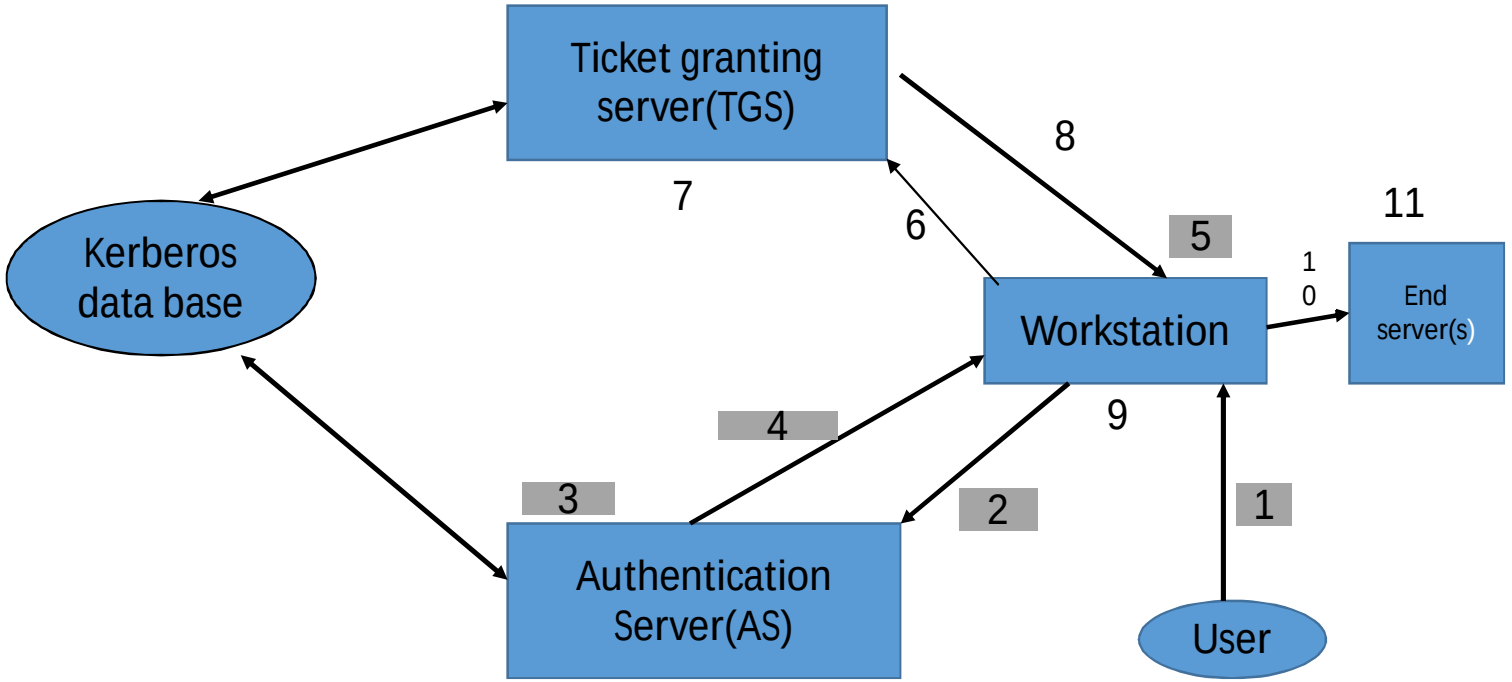
Kerberos

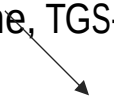



Ticket granting server(TGS)
Kerberos data base
Workstation
End server(s)
Authentication Server(AS)
User
1
2
3
4
5
6
7
8
9
10
11

Kerberos

1. User enters the login name in reponse to the prompt.
2. Message={ login-name,TGS-name}
3. The AS looks up the login-name and the service name in th ekerberos database.
4. Message={TGS-session key, sealed-ticket} →User's encryption key

   Ticket={ login-name, TGS-name,WS-netaddress,TGS-session key}

   TGS-server's encryption Key

5.He login program receives the encrypted message and only then prompts you for your password.

stores the sealed ticket, TGS-seesion key

----------User Authentication over----------

6.Workstation builds message={sealed-ticket, sealed-authenticator,end-serve name}

authenticator={ authenticator-login-name, WS-netaddress,current-time}

encrypted with TGS –Session key

7.The TGS-Server receives information compers the entities.if matches, obtains the encryption key for the specified service

8.TGS-Server builds the

Message={={New-session key, sealed-ticket} →**encrypted withTGS-Session key**

Ticket={ login-name, End server-name,WS-netaddress,New-session key}

Encrypted with End server Encryption key

9.The work station receives the message and decrypts with TGS-Session key

10.The work station builds the

message={sealed-ticket,sealed-authenticator,end-server name}

authenticator={ authenticator-login-name, WS-netaddress,current-time}

encrypts with new session key

11. The endserver receives this message and compare the entities, if matches grants the services