KERBEROS STEPS

KDC / Key Distribution Centre = (AS / Authentication Service, TGS / Ticket Granting Service)

Kkdc = TGS key = private key of KDC (must be protected) T/T2 = timestamps

Alice = Client Bob = Service Provider TGT = Ticket Granting Ticket

Kas = Alice/KDC shared key Kbs = Bob/KDC shared key

Kab = session key for use between Alice and Bob

* some of these steps involve 2 messages, shown here as one structure for ease of presentation.

1) The client Alice logs in with a password to local workstation which generates a copy of Kas, i.e. the principal key. The Key Distribution Centre - KDC is capable of generating Kas also (step 3). This is the shared secret Alice to KDC.

2) Alice sends a request in plaintext to the KDC requesting a TGT.

3) The KDC generates a time sensitive session key for Alice = Sa and a TGT = {Alice,Sa,T}K_{kdc}. The KDC returns to Alice {Sa, {Alice,Sa,T}K_{kdc}}Kas

4) Alice uses Kas to decrypt the response and extract Sa which will be used in subsequent communications with the KDC. The TGT = {Alice,Sa,T}K_{kdc} is not decipherable by Alice due to the use of the private Kkdc. Alice now requests a communication with Bob and sends a service ticket request along with the TGT and an authenticater to the KDC = {{Alice,Sa,T}K_{kdc},{Alice, IP, T}Sa, Bob } to the KDC. {Alice, IP, T}Sa is an authenticator for Alice.

5) The KDC examines the request from Alice and authenticates Alice by decoding the TGT with its private key K_{kdc} and extracting the Sa. The presence of Sa inside the TGT confirms Alice sent the authenticator as only Alice should have access to Sa from step 3. The KDC now generates a random service session key = Kab for Alice to Bob to use later and encrypts this and timestamp T inside the service using Kbs and returns these to Alice as {Bob,Kab,{Alice, Kab,T}Kbs}Sa
   * The KDC does not need to store session key Sa as it is inside the secure TGT when needed.

6) Alice uses Sa to open the response to get Kab and the unreadable service ticket for Bob = {Alice, Kab,T}Kbs, which also contains Kab, put there securely by the KDC.
   Alice sends a request to Bob for a service {Alice,{Alice, Kab,T}Kbs , {Alice,IP,T2} Kab}

7) The service Bob uses its Kbs to extract Kab from the service ticket which could only have been generated by the KDC. The Kab is then used to authenticate Alice by decrypting {Alice,IP,T2}, after a successful authentication Alice and Bob can establish a secure session using Kab. To prevent replay attacks T2+1 is sent in the return response as{T2+1}Kab. Bob may store a set of requests for a timeout window. May use Kab for secure communications if needed.

8) Alice validates T2+1, and can communicate with Bob

Note: Timestamps are checked to see if still valid i.e. recent, replay attacks within the window can be detected with a replay cache for of requests maintained over the window period (5 minutes).