



Ticket Granting Server has been setup with a password, the hash of the password has been used to determine a Ticket Granting Server key. This key is known to the authentication server.

Ticket Granting Service Exchange

Kerberos AP-REQ [Requests Ticket to Service]

The client now contacts the Ticket Granting Server for a ticket to access a Service. The client sends the authenticator, along with the TGT, to the TGS, requesting access to the target server. [Click on message name to see field level details.]

Ticket Granting Server authenticates the client

- SK1 = Decrypts with TGS key (TGT)
- Client Name, IP address, time stamp = Decrypt with Session Key SK1 (Authenticator)
- Verify that the IP address in the Authenticator matches the Client's IP address from the received message
- Check from the timestamp that the 'Ticket Granting Ticket' has not expired
- Check Client permissions to determine if the user is allowed to access the requested service

Ticket Granting Server decrypts the 'Ticket Granting Ticket' with the TGS key. The Session Key SK1 is extracted from the TGT.

TGS then uses the SK1 inside the TGT to decrypt the authenticator and extract Client Name, IP Address and timestamp.

TGS generates ticket for service

- Service Session Key SK2
- Lookup Service Master Key
- Service Ticket = Encrypt with Service Master Key [Service Session Key SK2, Client Name, IP Address, Timestamp]
- TGS-RES Body = Encrypt with Session Key SK1 (Service Session Key SK2, Service Ticket)

Generate a Service Session Key SK2 for the service session.

Lookup the key database to find the Service Master Key for the requested service (File Server in this case).

Form the Service Ticket from the Client Name, Client IP, Timestamp and the Service Session Key SK2. The Service ticket is encrypted with the Service Master Key for the server offering the service.

The message body is encrypted with SK1 what is known to the Client. Note that in this arrangement, the Client Master Key has been used to initially establish the session. Once the session is established, just the session key is used for ciphering.

Kerberos TGS-REP [Service Ticket for File Server Access]

The TGS sends the encrypted SK2 and the Service Ticket to the Client. [Click on message name to see field level details.]

Ticket Granting Server Interfaces (Get a Ticket Granting Ticket then Use it to Obtain a Service Ticket)

| | | | | |
|--------|----------------------------------|----------------------------|---------------------------|-------------------------------|
| User | Kerberos Key Distribution Center | | | EventStudio System Designer 6 |
| Client | Authentication Server | Service Session Key SK2 | Ticket Granting Server | 10-Dec-14 08:18 (Page 2) |

