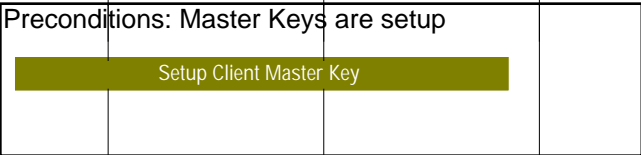


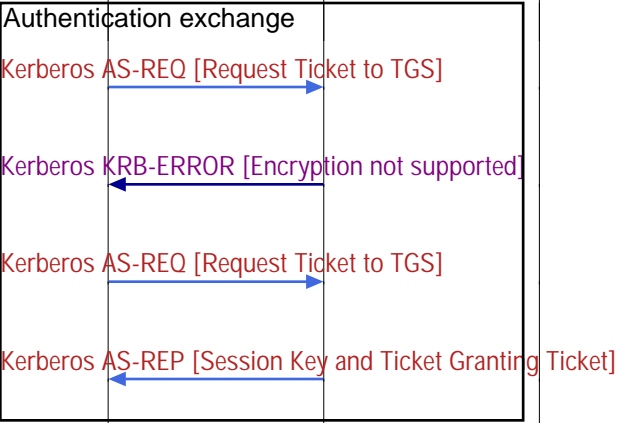
**Component Interfaces (Get a Ticket Granting Ticket then Use it to Obtain a Service Ticket)**



User has setup a password, the hash of the password has been used to determine a client user key. This key is known to the authentication server

**User Logs in with the Password**

User logs into the account.

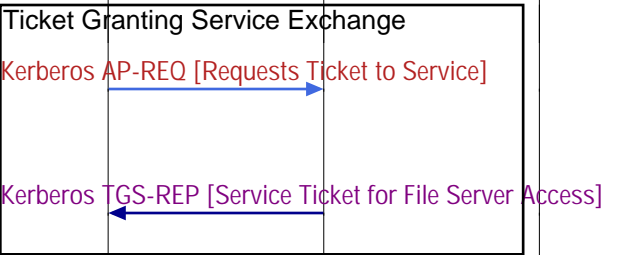


The client asks the Authentication Server for a ticket to the Ticket Granting Server (TGS). [Click on message name to see field level details.]

The Authentication Server does not support the requested authentication. The server responds back to the client with supported authentication modes. [Click on message name to see field level details.]

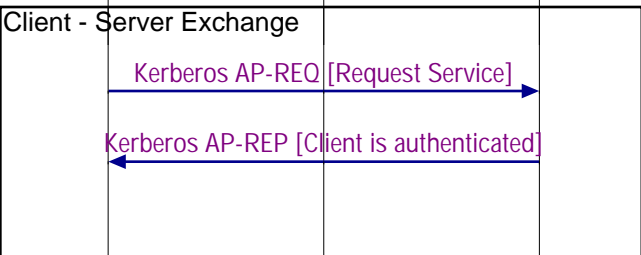
The client resends a request to the authentication server for a ticket to the Authentication Server with the requested encryption type. [Click on message name to see field level details.]

The ticket granting ticket (TGT) is sent to the Client. [Click on message name to see field level details.]



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.]

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



The client sends the authenticator and the service ticket to the "File Server"

The File Server has returned a message consisting of the time stamp plus 1, encrypted with SK2. This proves to the client that the server actually knew its own secret key and thus could decrypt the ticket and the authenticator.