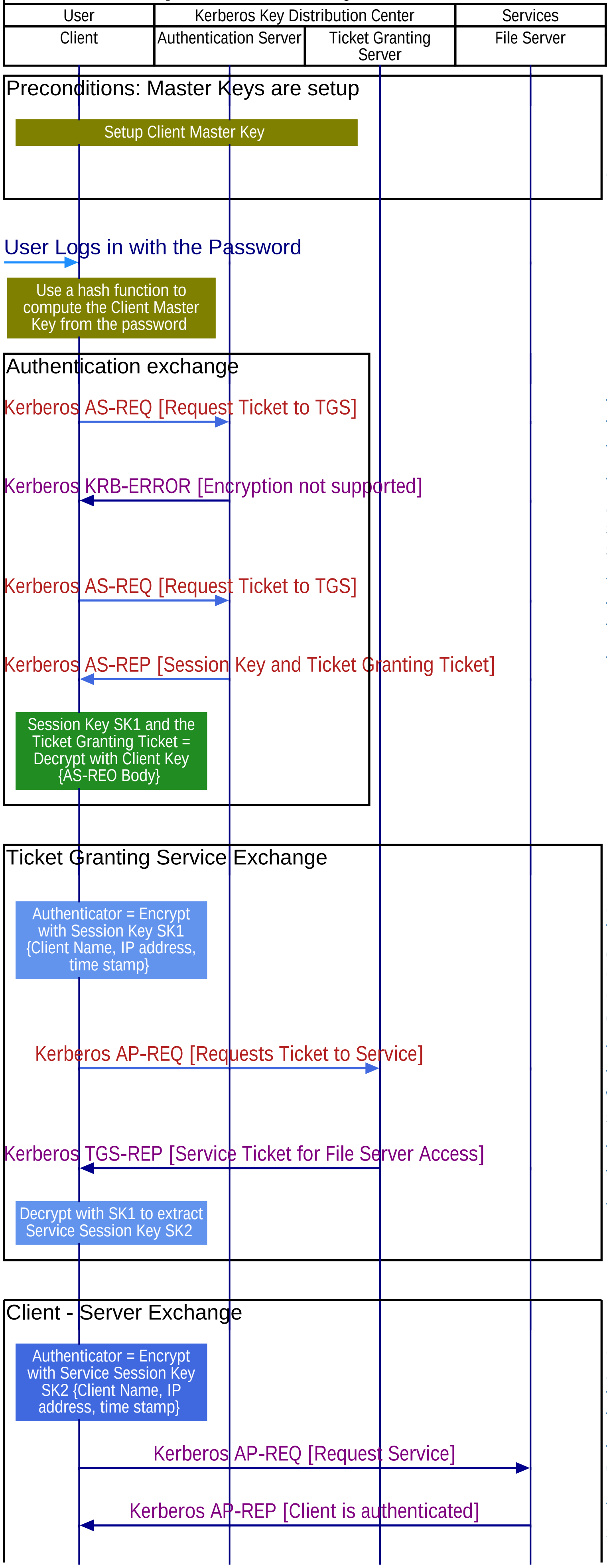
Client Interfaces (Get a Ticket Granting Ticket then Use it to Obtain a Service Ticket)


User
Kerberos Key Distribution Center
Services
Client
Authentication Server
Ticket Granting Server
File Server
Preconditions: Master Keys are setup
Setup Client Master Key
User Logs in with the Password
Use a hash function to compute the Client Master Key from the password
Authentication exchange
Kerberos AS-REQ [Request Ticket to TGS]
Kerberos KRB-ERROR [Encryption not supported]
Kerberos AS-REQ [Request Ticket to TGS]
Kerberos AS-REP [Session Key and Ticket Granting Ticket]
Session Key SK1 and the Ticket Granting Ticket = Decrypt with Client Key {AS-REO Body}
Ticket Granting Service Exchange
Authenticator = Encrypt with Session Key SK1 {Client Name, IP address, time stamp}
Kerberos AP-REQ [Requests Ticket to Service]
Kerberos TGS-REP [Service Ticket for File Server Access]
Decrypt with SK1 to extract Service Session Key SK2
Client - Server Exchange
Authenticator = Encrypt with Service Session Key SK2 {Client Name, IP address, time stamp}
Kerberos AP-REQ [Request Service]
Kerberos AP-REP [Client is authenticated]

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 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.]

Decrypt the message with the Client key and extract Session Key SK1 and Ticket Granting Ticket.

In this example, the Client wishes to get a ticket to a File Server.

Generate the authenticator to validate the client to the TGS. The authenticator is encrypted with the Session Key SK1. This encryption is used as a proof of authenticity at the TGS. The Client extracted the SK1 from a message encrypted with the Client Master Key. The TGS will extract SK1 from the TGT by decrypting it with the TGT Master Key.

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 Service Session Key SK2 is extracted at the client.

Generate the authenticator for the service. Encrypt the authenticator with the Service Session Key SK2. The encrypted time stamp prevents an eavesdropper from recording both the ticket and authenticator and replaying them later.

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

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

User	Kerberos Key Distribution Center		Services
Client	Authentication Server	Ticket Granting Server	File Server

the server actually knew its own secret key and thus could decrypt the ticket and the authenticator.