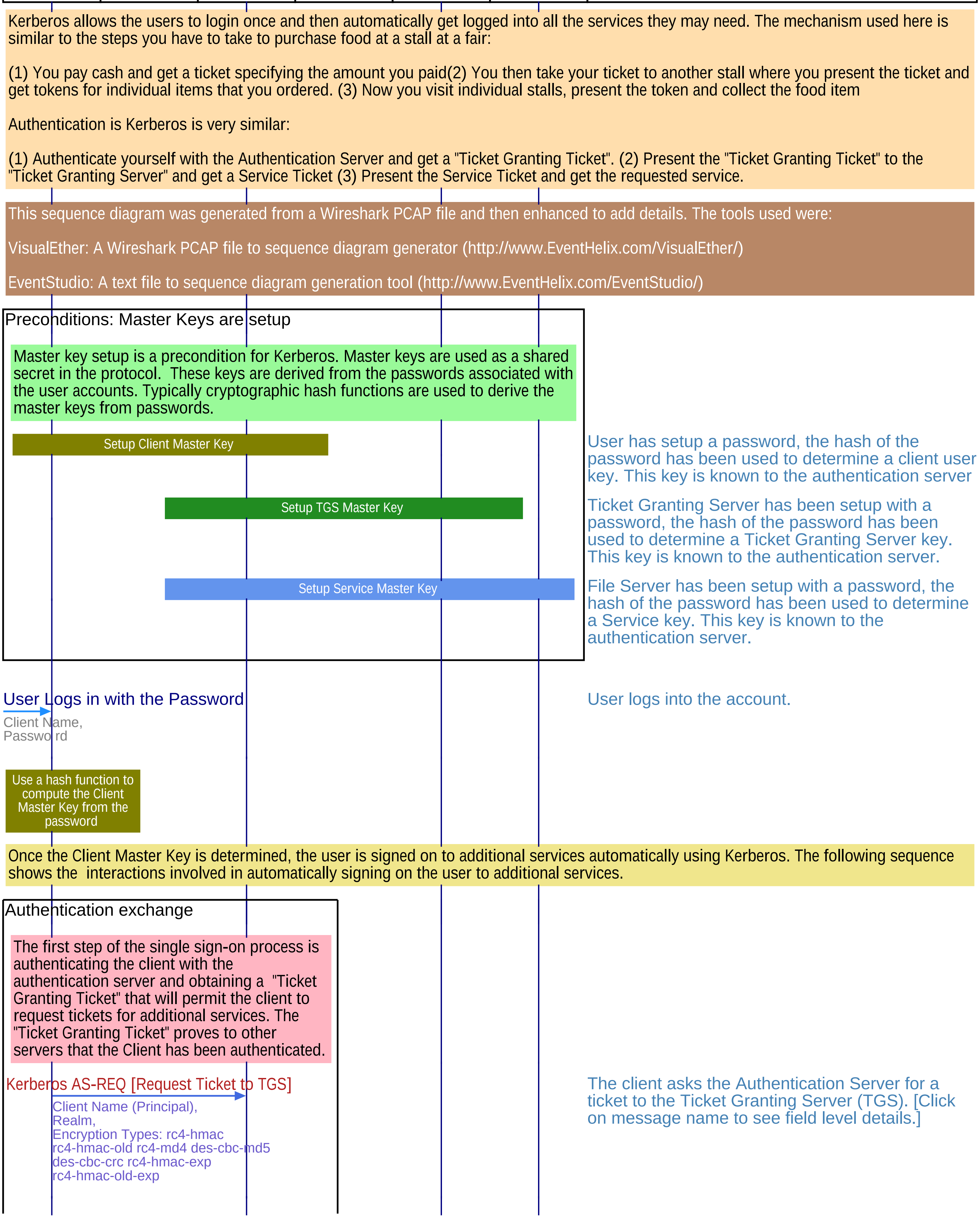
Single Sign On with Kerberos (Get a Ticket Granting Ticket then Use it to Obtain a Service Ticket)

User	Kerberos Key Distribution Center				Services	EventStudio System Designer 6
Client		Authentication Server		Ticket Granting Server	File Server	10-Dec-14 08:18 (Page 1)



Kerberos allows the users to login once and then automatically get logged into all the services they may need. The mechanism used here is similar to the steps you have to take to purchase food at a stall at a fair:

(1) You pay cash and get a ticket specifying the amount you paid(2) You then take your ticket to another stall where you present the ticket and get tokens for individual items that you ordered. (3) Now you visit individual stalls, present the token and collect the food item

Authentication is Kerberos is very similar:

(1) Authenticate yourself with the Authentication Server and get a "Ticket Granting Ticket". (2) Present the "Ticket Granting Ticket" to the "Ticket Granting Server" and get a Service Ticket (3) Present the Service Ticket and get the requested service.

This sequence diagram was generated from a Wireshark PCAP file and then enhanced to add details. The tools used were:

VisualEther: A Wireshark PCAP file to sequence diagram generator (http://www.EventHelix.com/VisualEther/)

EventStudio: A text file to sequence diagram generation tool (http://www.EventHelix.com/EventStudio/)

Preconditions: Master Keys are setup

Master key setup is a precondition for Kerberos. Master keys are used as a shared secret in the protocol. These keys are derived from the passwords associated with the user accounts. Typically cryptographic hash functions are used to derive the master keys from passwords.

Setup Client Master Key

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

Setup TGS Master Key

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.

Setup Service Master Key

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

User Logs in with the Password

Client Name,
Password

User logs into the account.

Use a hash function to compute the Client Master Key from the password

Once the Client Master Key is determined, the user is signed on to additional services automatically using Kerberos. The following sequence shows the interactions involved in automatically signing on the user to additional services.

Authentication exchange

The first step of the single sign-on process is authenticating the client with the authentication server and obtaining a "Ticket Granting Ticket" that will permit the client to request tickets for additional services. The "Ticket Granting Ticket" proves to other servers that the Client has been authenticated.

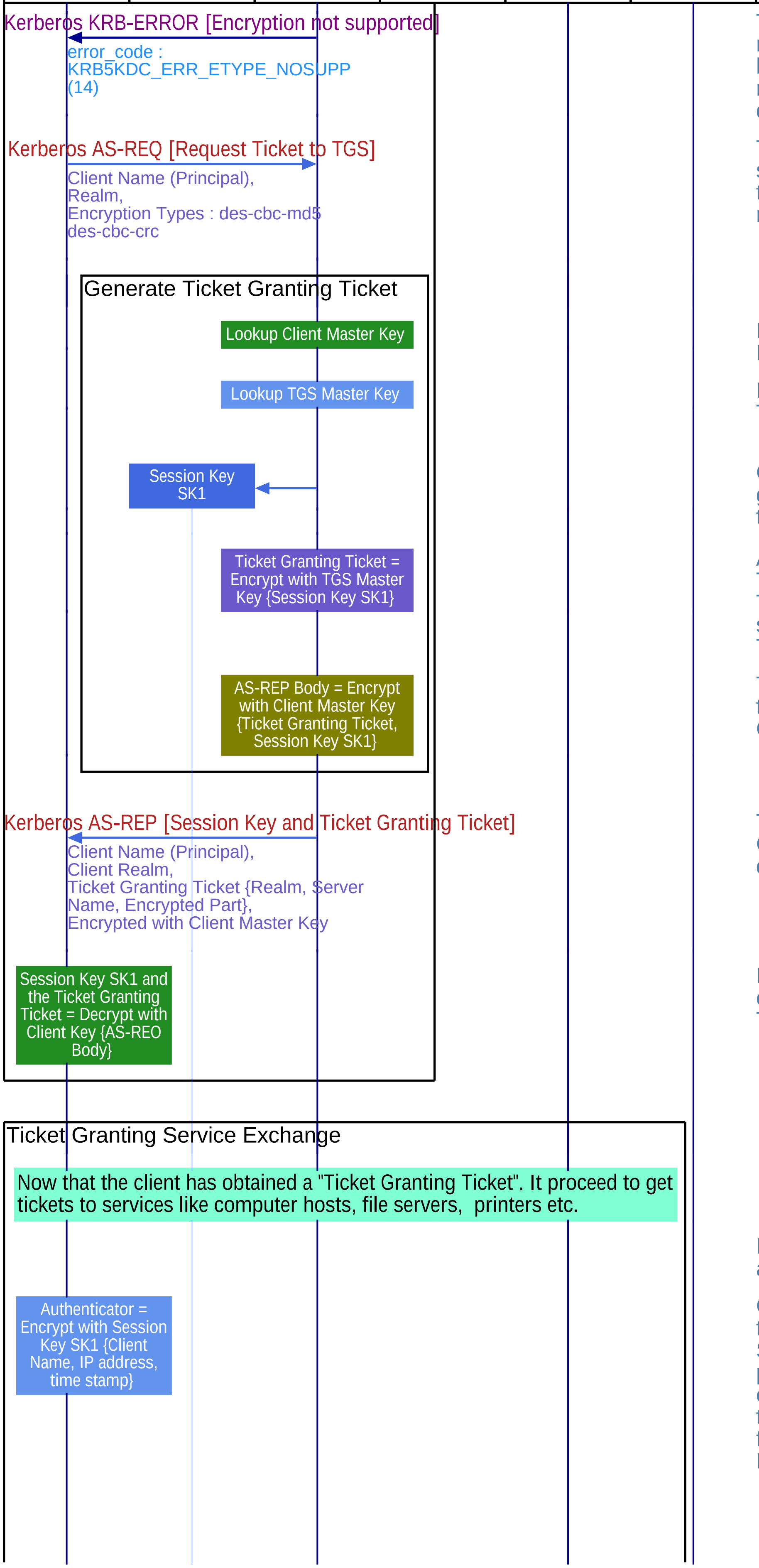
Kerberos AS-REQ [Request Ticket to TGS]

Client Name (Principal),
Realm,
Encryption Types: rc4-hmac
rc4-hmac-old rc4-md4 des-cbc-md5
des-cbc-crc rc4-hmac-exp
rc4-hmac-old-exp

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

Single Sign On with Kerberos (Get a Ticket Granting Ticket then Use it to Obtain a Service Ticket)

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



Kerberos KRB-ERROR [Encryption not supported]

error_code : KRB5KDC_ERR_ETYPE_NOSUPP (14)

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.]

Kerberos AS-REQ [Request Ticket to TGS]

Client Name (Principal),
Realm,
Encryption Types : des-cbc-md5
des-cbc-crc

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.]

Generate Ticket Granting Ticket

Lookup Client Master Key

Lookup database for the Client to find the Client Master Key.

Lookup TGS Master Key

Lookup database for the TGS Server to find the TGS Master Key.

Session Key SK1

Client is found so the Authentication Server generates a session key (SK1) for use between the client and the TGS.

Ticket Granting Ticket = Encrypt with TGS Master Key {Session Key SK1}

Authentication Server generates a Ticket Granting Ticket. The ticket contains the Session Key SK1. The ticket is encrypted with the TGS Master Key, so it's contents can only be deciphered by the TGS.

AS-REP Body = Encrypt with Client Master Key {Ticket Granting Ticket, Session Key SK1}

The body for the response is finally encrypted with the Client Master Key. This ensures that only the Client can decode this message.

Kerberos AS-REP [Session Key and Ticket Granting Ticket]

Client Name (Principal),
Client Realm,
Ticket Granting Ticket {Realm, Server Name, Encrypted Part},
Encrypted with Client Master Key

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

Session Key SK1 and the Ticket Granting Ticket = Decrypt with Client Key {AS-REO Body}

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

Ticket Granting Service Exchange

Now that the client has obtained a "Ticket Granting Ticket". It proceed to get tickets to services like computer hosts, file servers, printers etc.

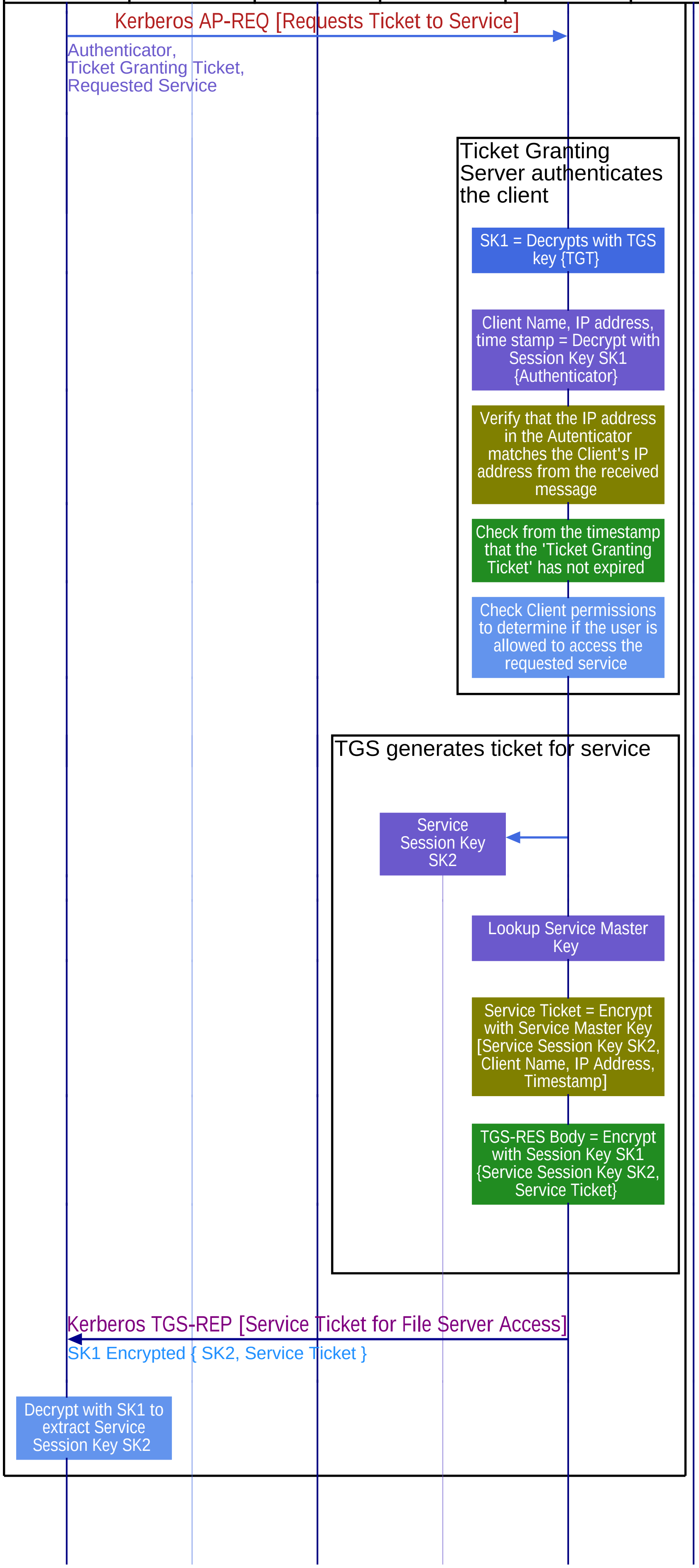
In this example, the Client wishes to get a ticket to a File Server.

Authenticator = Encrypt with Session Key SK1 {Client Name, IP address, time stamp}

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.

Single Sign On with Kerberos (Get a Ticket Granting Ticket then Use it to Obtain a Service Ticket)

User	Kerberos Key Distribution Center				Services	**EventStudio System Designer 6**
Client	Session Key SK1	Authentication Server		Ticket Granting Server	File Server	10-Dec-14 08:18 (Page 3)



Kerberos AP-REQ [Requests Ticket to Service]

Authenticator,
Ticket Granting Ticket,
Requested 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}

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

Client Name, IP address, time stamp = Decrypt with Session Key SK1 {Authenticator}

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

Verify that the IP address in the Autenticator 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

TGS generates ticket for service

Service Session Key SK2

Generate a Service Session Key SK2 for the service session.

Lookup Service Master Key

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

Service Ticket = Encrypt with Service Master Key [Service Session Key SK2, Client Name, IP Address, Timestamp]

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.

TGS-RES Body = Encrypt with Session Key SK1 {Service Session Key SK2, Service Ticket}

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]

SK1 Encrypted { SK2, Service Ticket }

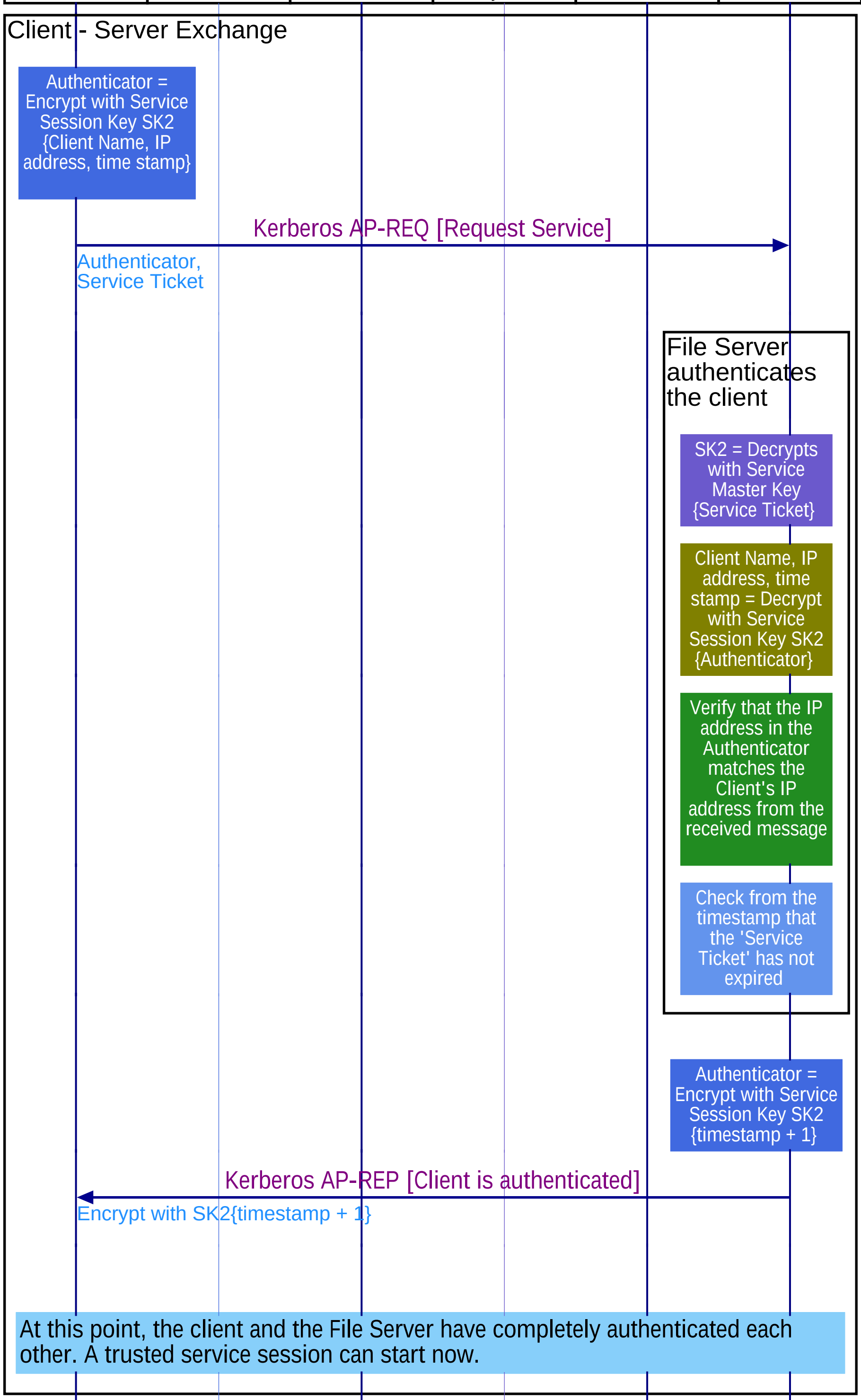
The TGS sends the encrypted SK2 and the Service Ticket to the Client. [Click on message name to see field level details.]

Decrypt with SK1 to extract Service Session Key SK2

The Service Session Key SK2 is extracted at the client.

Single Sign On with Kerberos (Get a Ticket Granting Ticket then Use it to Obtain a Service Ticket)

User	Kerberos Key Distribution Center				Services	EventStudio System Designer 6
Client	Session Key SK1	Authentication Server	Service Session Key SK2	Ticket Granting Server	File Server	10-Dec-14 08:18 (Page 4)



Client - Server Exchange

Authenticator = Encrypt with Service Session Key SK2 {Client Name, IP address, time stamp}

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.

Kerberos AP-REQ [Request Service]

Authenticator, Service Ticket

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

File Server authenticates the client

SK2 = Decrypts with Service Master Key {Service Ticket}

The File Server decrypts the 'Service Ticket' with the Service Master Key. The Session Key SK2 is extracted from the Service Ticket.

Client Name, IP address, time stamp = Decrypt with Service Session Key SK2 {Authenticator}

The File Server then uses the SK2 inside the Service Ticket to decrypt the authenticator and extract Client Name, IP Address and timestamp.

Verify that the IP address in the Authenticator matches the Client's IP address from the received message

Check from the timestamp that the 'Service Ticket' has not expired

Authenticator = Encrypt with Service Session Key SK2 {timestamp + 1}

The File Server adds 1 to the received timestamp and encrypts it with SK2.

Kerberos AP-REP [Client is authenticated]

Encrypt with SK2{timestamp + 1}

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.

At this point, the client and the File Server have completely authenticated each other. A trusted service session can start now.

Explore More:

TCP/IP Sequence Diagrams http://www.EventHelix.com/RealtimeMantra/Networking/

VisualEther: A Wireshark PCAP file to sequence diagram generator http://www.EventHelix.com/VisualEther/

EventStudio: A text file to sequence diagram generation tool http://www.EventHelix.com/EventStudio/