Section 1

- Kerberos is a network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner .

- The authentication is based on tickets used as credentials, allowing communication and proving identity over a non-secure networking net .

- The three-heads of Kerbero are: 1-User, 2-KDC-Key Distribution Service (security server) and 3-Services .

In Greek mythology, a many headed dog, the guardian of the entrance of Hades

Characteristics of Kerberos

- For all services that rely on Kerberos for access control, lack of availability of the service means lack of support for the supported services .

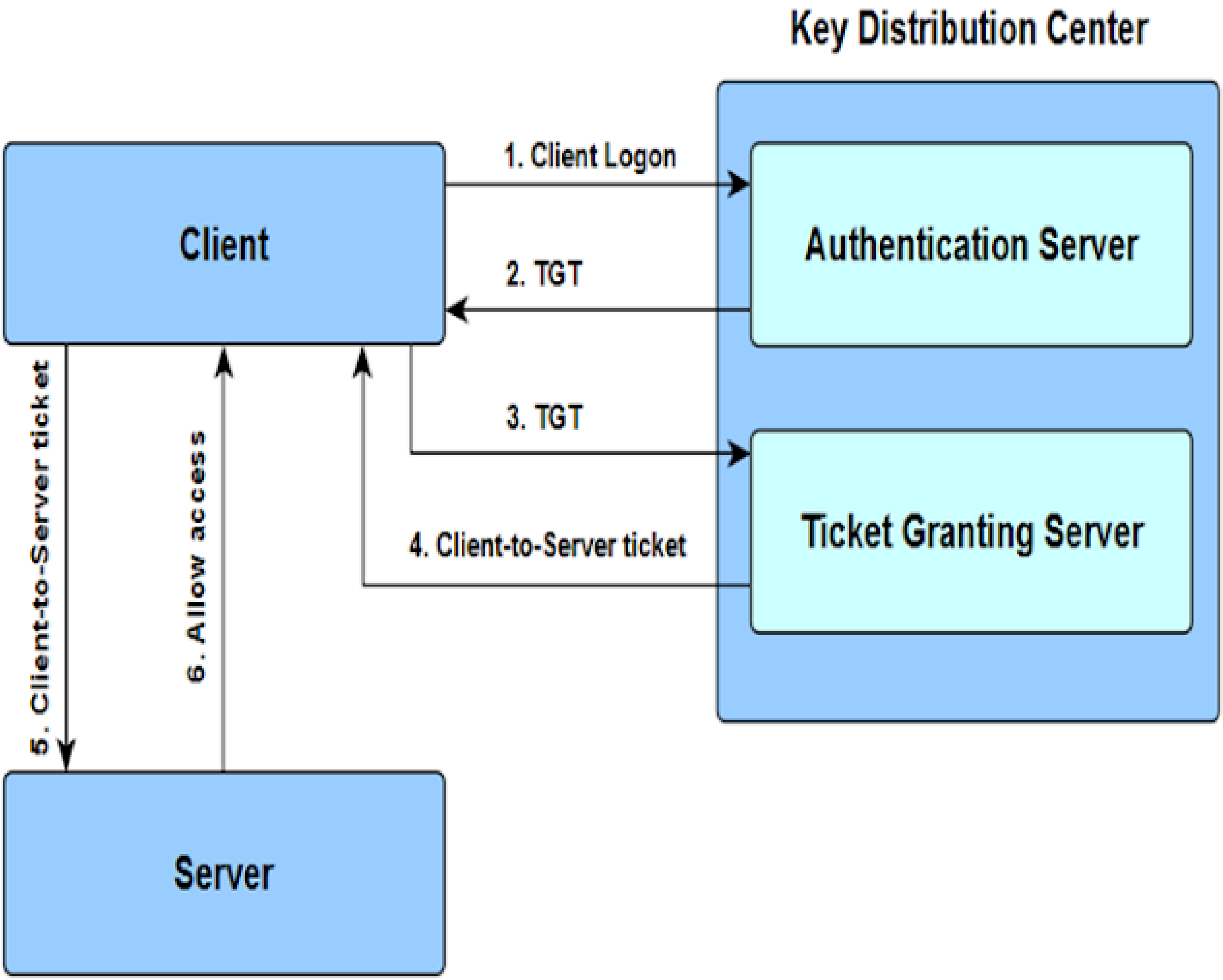
- This suggests a modular, distributed architecture, with one system able to back up another .

Kerberos Protocol Terminology

- Client: An entity on the network that can receive a ticket from Kerberos .

- Credentials: A temporary set of electronic credentials that verify the identity of a client for a particular service .

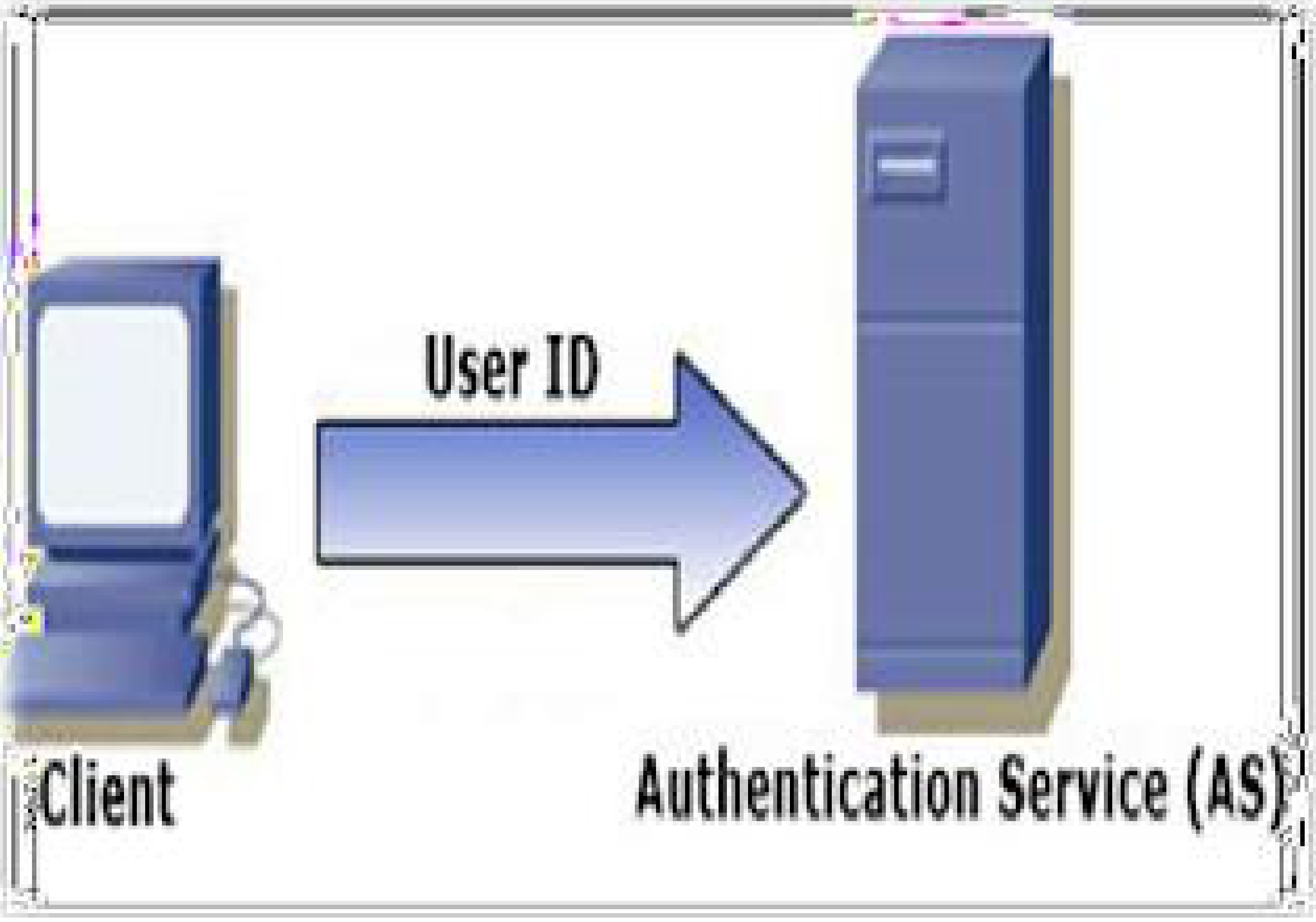
- Ticket-granting server (TGS) is a server that issues tickets for a desired service which are in turn given to users .

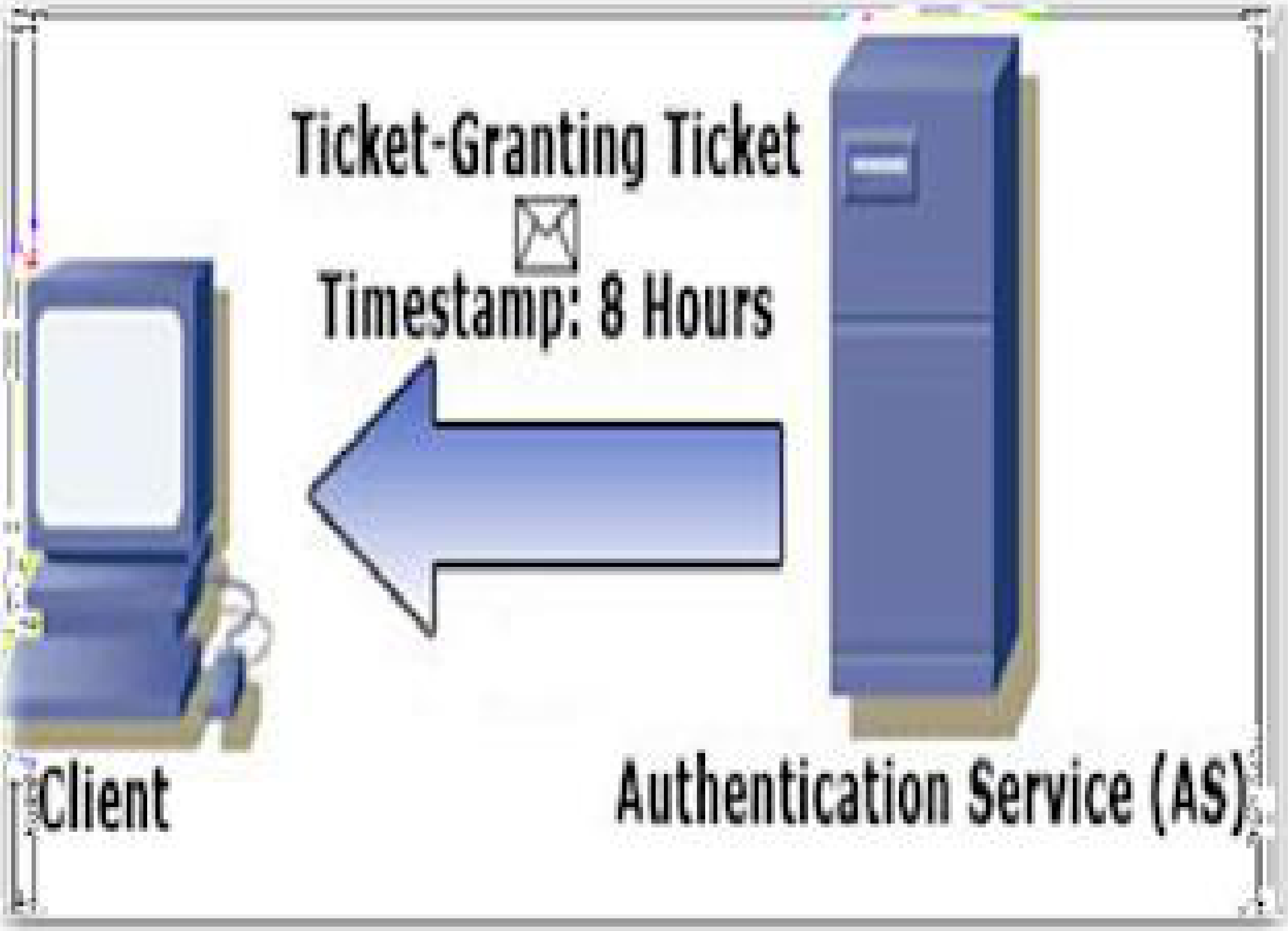


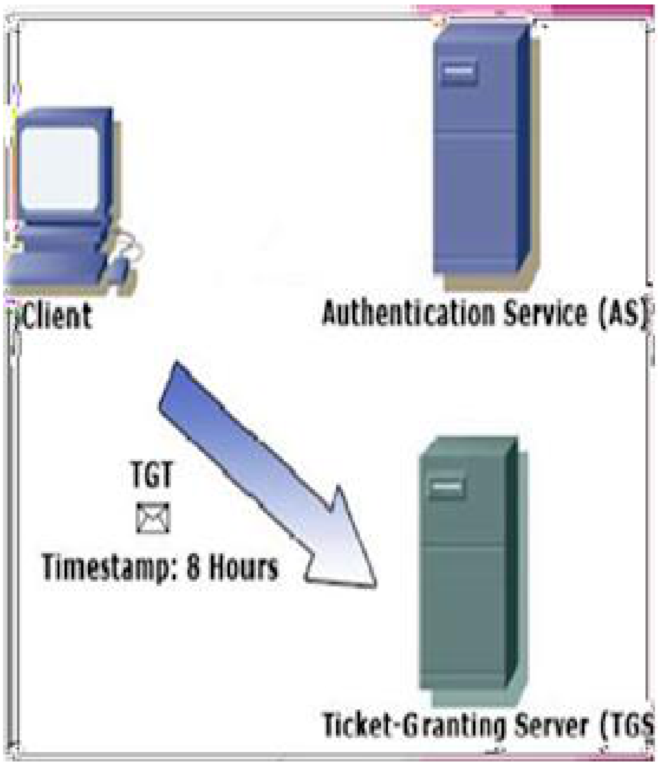
Working of Kerberos

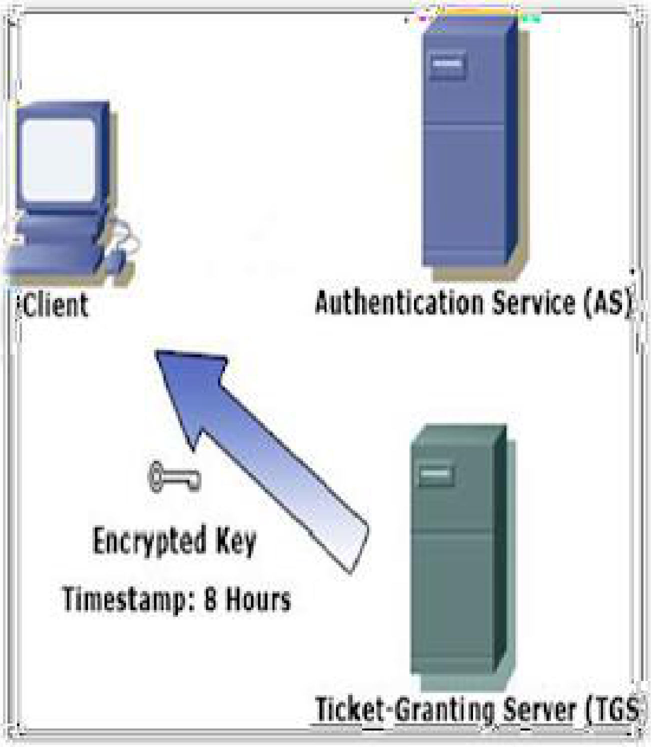
- Kerberos is a network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner .

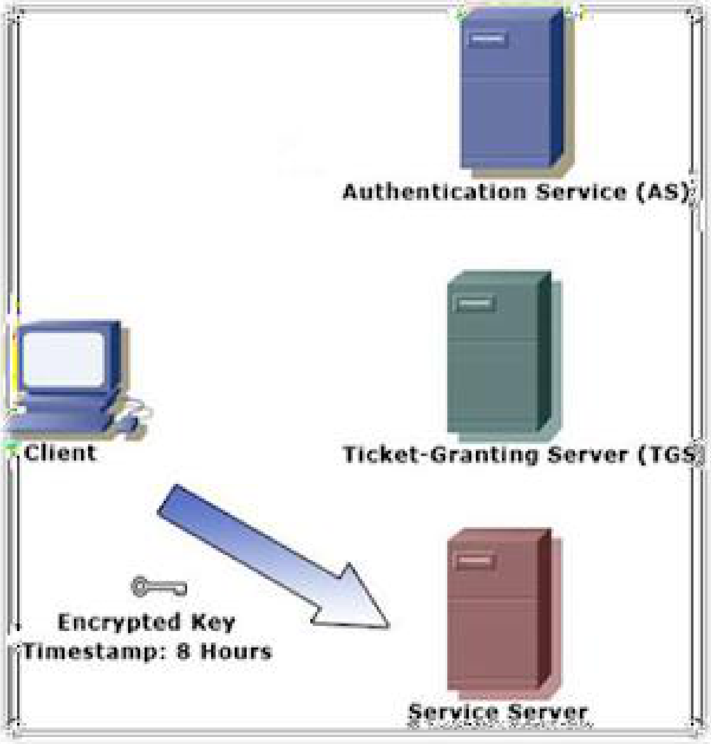
- It does not send plain text pass-words over the network and instead of password uses encrypted tickets .

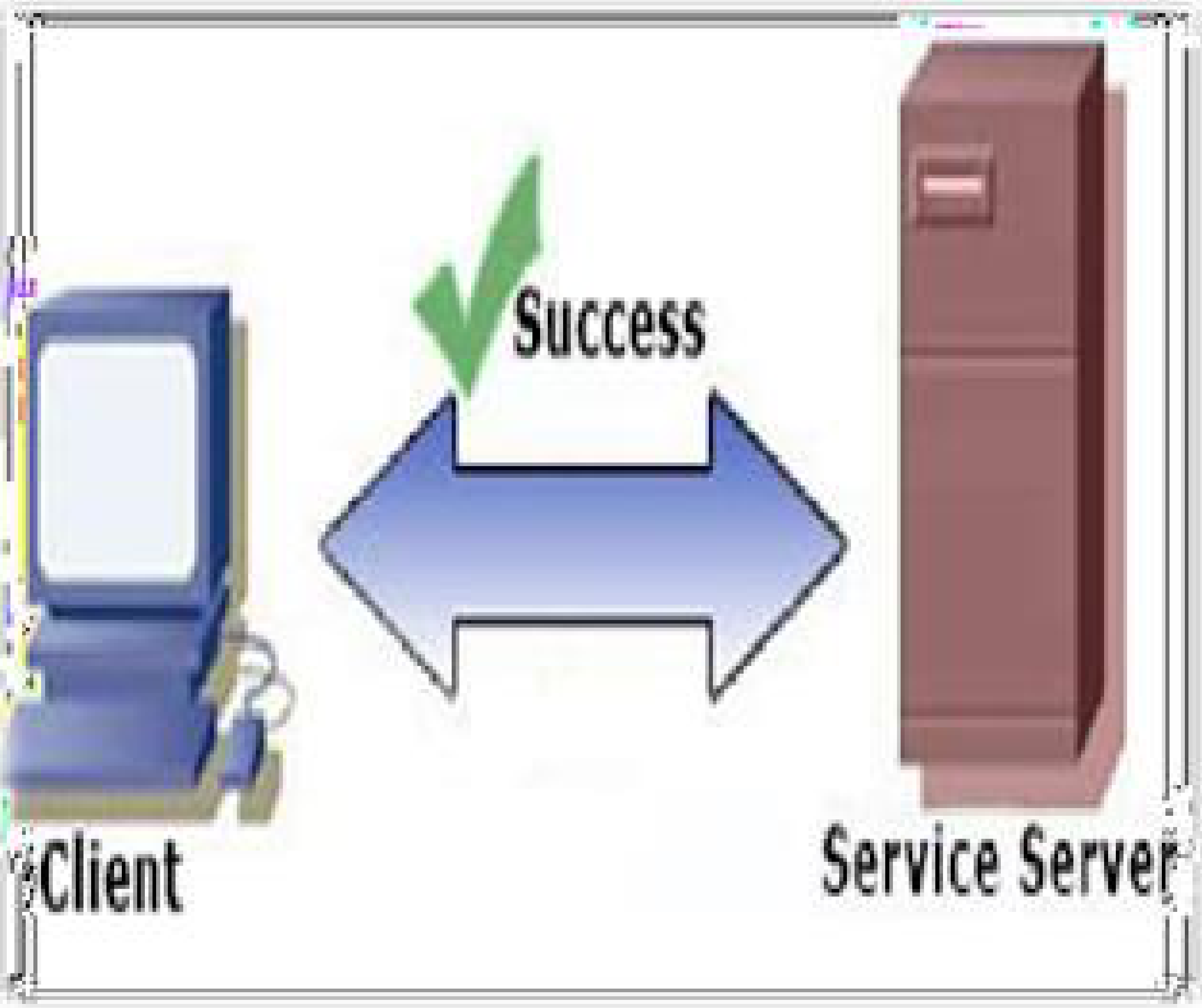

User ID
Client
Authentication Service (AS)


Ticket-Granting Ticket
Timestamp: 8 Hours
Client
Authentication Service (AS)


Client
Authentication Service (AS)
TGT
Timestamp: 8 Hours
Ticket-Granting Server (TGS

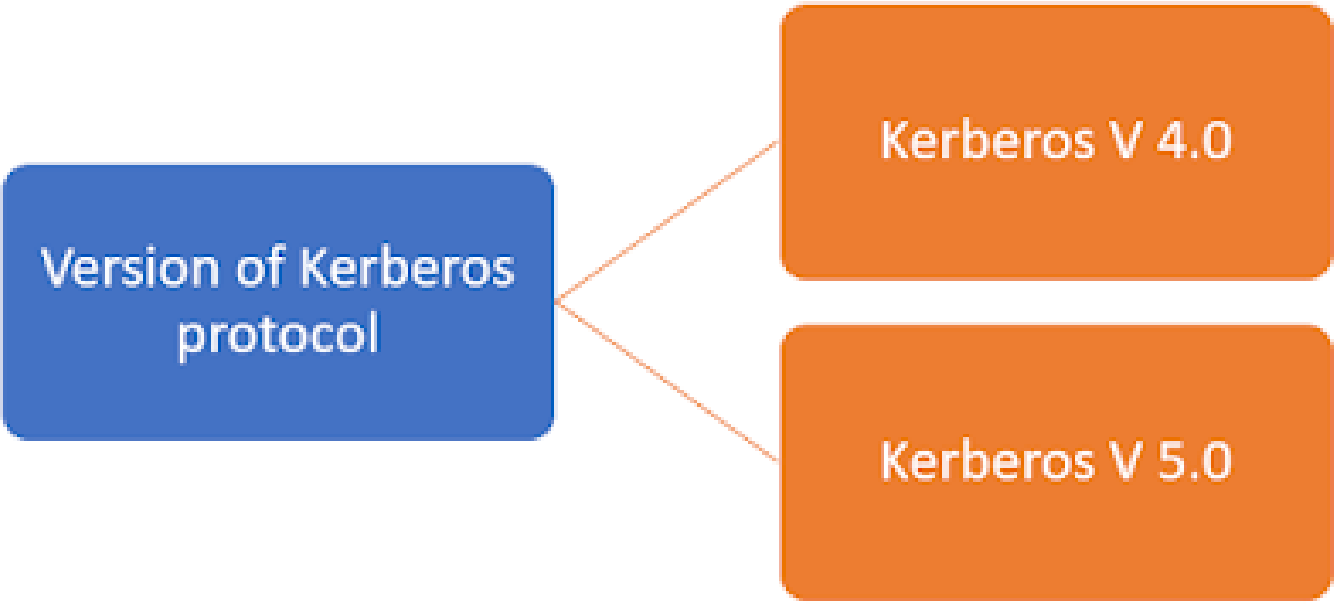

Client
Authentication Service (AS)
Encrypted Key
Timestamp: 8 Hours
Ticket-Granting Server (TGS


Authentication Service (AS)
Client
Ticket-Granting Server (TGS)
Encrypted Key
Timestamp: 8 Hours
Service Server


Success
Client
Service Server

Different Version of Kerberos Protocols

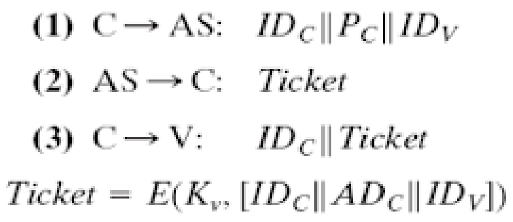
- Using Authentication Server (AS) and Ticket Granting Server (TGS) are different schemes .
- In these schemes, password is transmitted without encryption .
- An adversary could capture the password and use any service accessible to the victim .
- The client transmits a message to the TGS containing the user's ID, the ID of the desired service, and the ticket-granting ticket .
- Step - 4: The TGS decrypts the incoming ticket using Ktgs and verifies the success of the decryption by the presence of its ID .



Version of Kerberos protocol

Kerberos V 4.0

Kerberos V 5.0

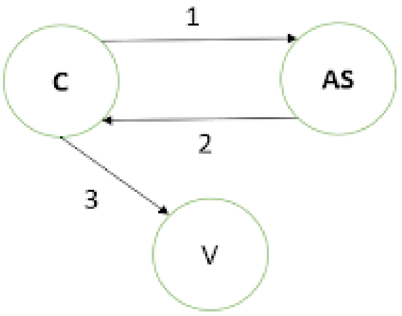


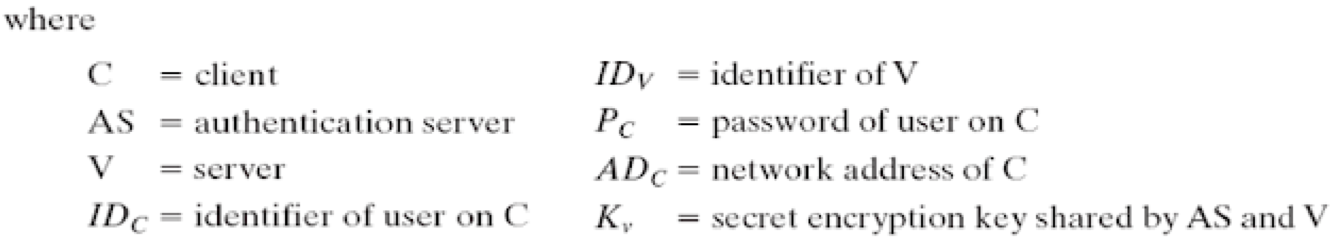
(1) C → AS: $ID_C \| P_C \| ID_V$

(2) AS → C: $Ticket$

(3) C → V: $ID_C \| Ticket$

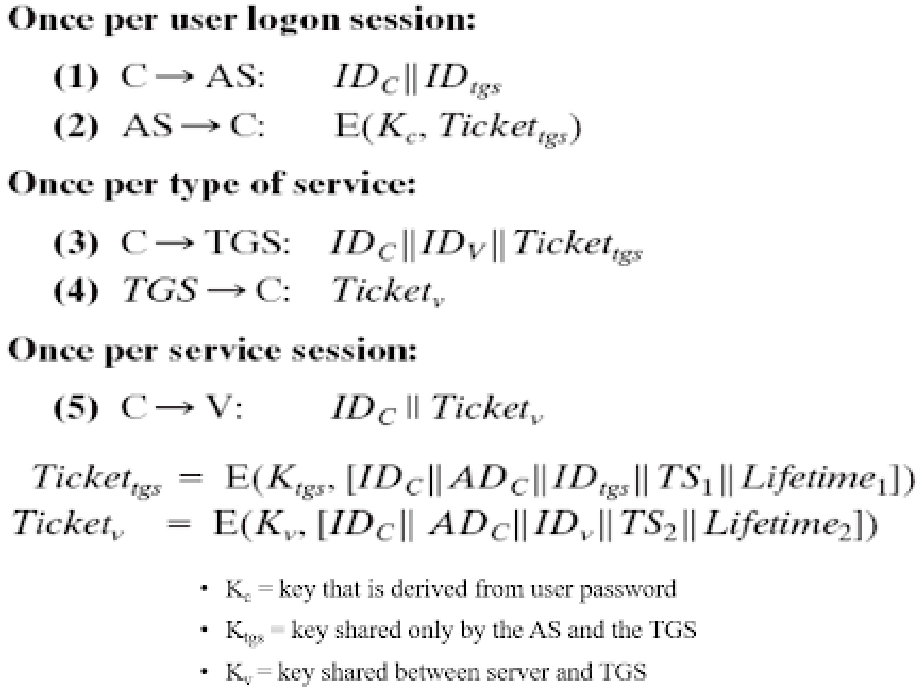
$$Ticket = E(K_v, [ID_C \| AD_C \| ID_V])$$





where

C	= client	ID_V	= identifier of V
AS	= authentication server	P_C	= password of user on C
V	= server	AD_C	= network address of C
ID_C	= identifier of user on C	K_v	= secret encryption key shared by AS and V



Once per user logon session:

(1) $C \rightarrow AS$: $ID_C \| ID_{tgs}$

(2) $AS \rightarrow C$: $E(K_c, Ticket_{tgs})$

Once per type of service:

(3) $C \rightarrow TGS$: $ID_C \| ID_V \| Ticket_{tgs}$

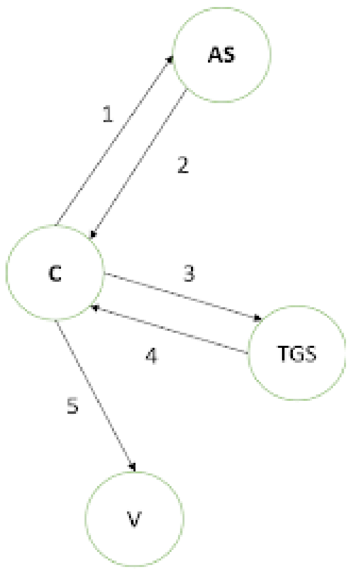
(4) $TGS \rightarrow C$: $Ticket_v$

Once per service session:

(5) $C \rightarrow V$: $ID_C \| Ticket_v$

$$Ticket_{tgs} = E(K_{tgs}, [ID_C \| AD_C \| ID_{tgs} \| TS_1 \| Lifetime_1])$$
$$Ticket_v = E(K_v, [ID_C \| AD_C \| ID_v \| TS_2 \| Lifetime_2])$$

- K_c = key that is derived from user password
- K_{tgs} = key shared only by the AS and the TGS
- K_v = key shared between server and TGS



Problems

- A network service (the TGS or an application service) must be properable to prove that the person using a ticket is the same person to whom that ticket was issued .

- Problem - 2: There may be a requirement for servers to authenticate themselves to users .

- Without such authentication, the false server would then be in a position to act as a real server and capture any information from the user .

Solution

- AS provides both the client and the TGS with a secret piece of information in a secure manner .

- Then the client can prove its identity to the TGS by revealing the secret information .

- An efficient way of accomplishing this is to use an encryption key as the secure information .

Kerberos Version 4 Message Exchange Scenario

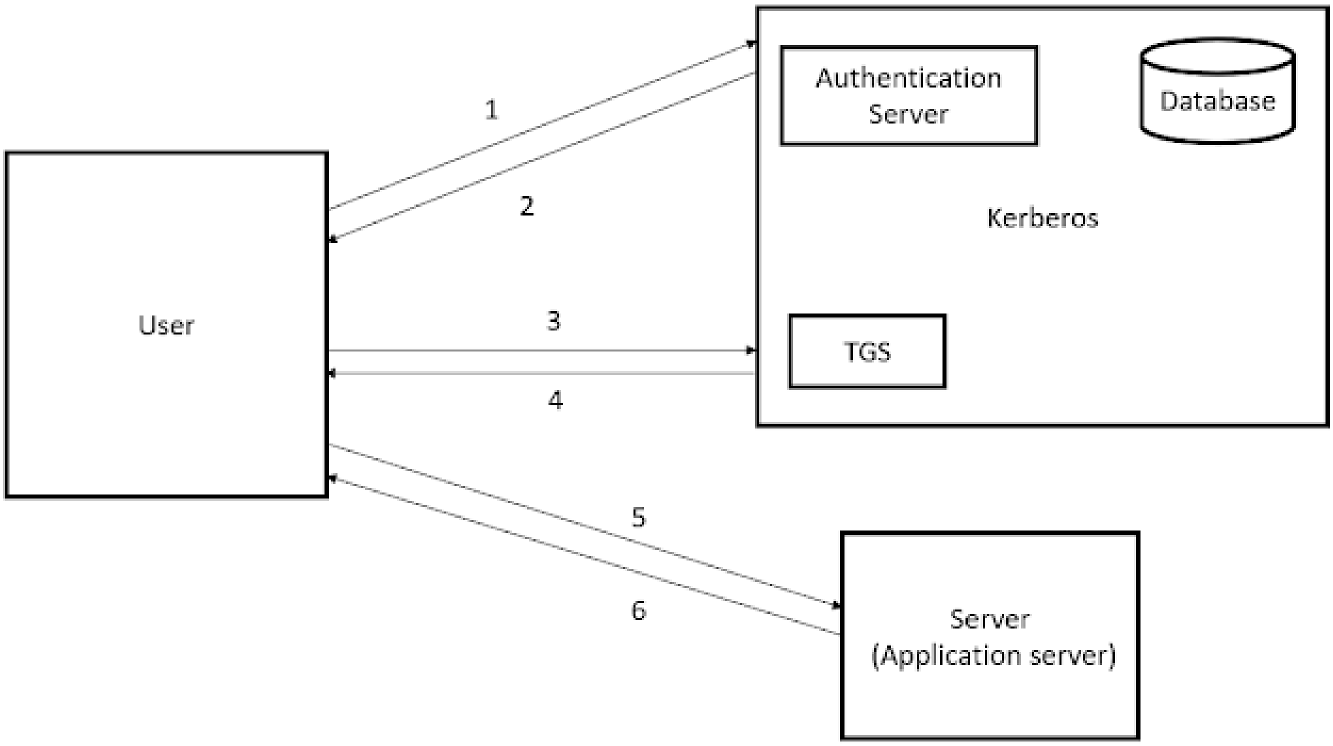
- The client sends a message to the AS requesting access to the TGS .

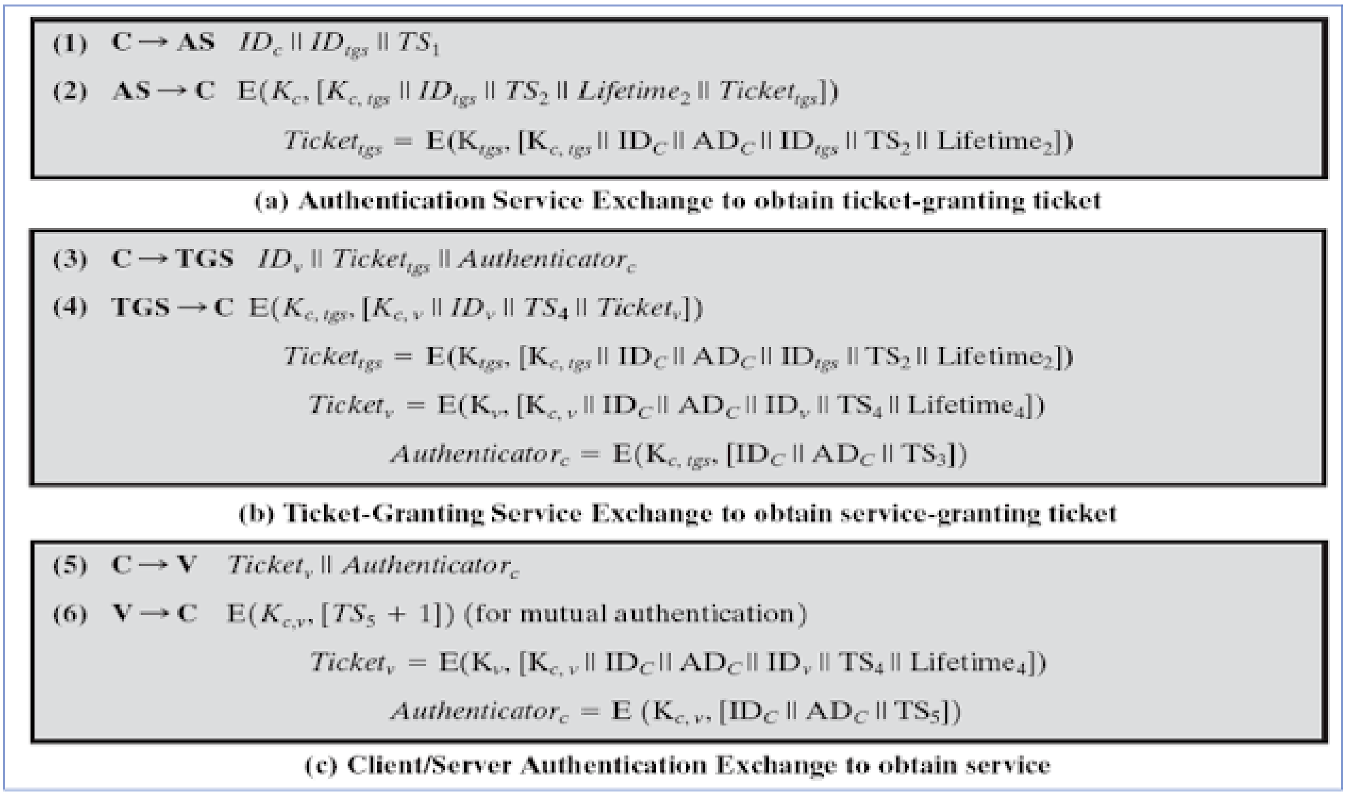
- The AS responds with a message encrypted with a key derived from the user's password (KC), that contains the ticket .

- The encrypted message also contains a copy of the session key, KC, tgs, where the subscripts indicate that this is a session key for C and TGS.

- C transmits an authenticator, which includes the ID and address of the user and a timestamp .

- The TGS can then check the name and address with that of the ticket and with the network





(1) $\mathbf{C \rightarrow AS}$ $ID_c \,||\, ID_{tgs} \,||\, TS_1$

(2) $\mathbf{AS \rightarrow C}$ $E(K_c, [K_{c,tgs} \,||\, ID_{tgs} \,||\, TS_2 \,||\, Lifetime_2 \,||\, Ticket_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \,||\, ID_C \,||\, AD_C \,||\, ID_{tgs} \,||\, TS_2 \,||\, Lifetime_2])$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) $\mathbf{C \rightarrow TGS}$ $ID_v \,||\, Ticket_{tgs} \,||\, Authenticator_c$

(4) $\mathbf{TGS \rightarrow C}$ $E(K_{c,tgs}, [K_{c,v} \,||\, ID_v \,||\, TS_4 \,||\, Ticket_v])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \,||\, ID_C \,||\, AD_C \,||\, ID_{tgs} \,||\, TS_2 \,||\, Lifetime_2])$

$Ticket_v = E(K_v, [K_{c,v} \,||\, ID_C \,||\, AD_C \,||\, ID_v \,||\, TS_4 \,||\, Lifetime_4])$

$Authenticator_c = E(K_{c,tgs}, [ID_C \,||\, AD_C \,||\, TS_3])$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

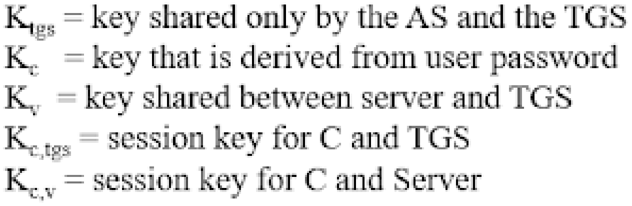
(5) $\mathbf{C \rightarrow V}$ $Ticket_v \,||\, Authenticator_c$

(6) $\mathbf{V \rightarrow C}$ $E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$Ticket_v = E(K_v, [K_{c,v} \,||\, ID_C \,||\, AD_C \,||\, ID_v \,||\, TS_4 \,||\, Lifetime_4])$

$Authenticator_c = E\,(K_{c,v}, [ID_C \,||\, AD_C \,||\, TS_5])$

(c) Client/Server Authentication Exchange to obtain service

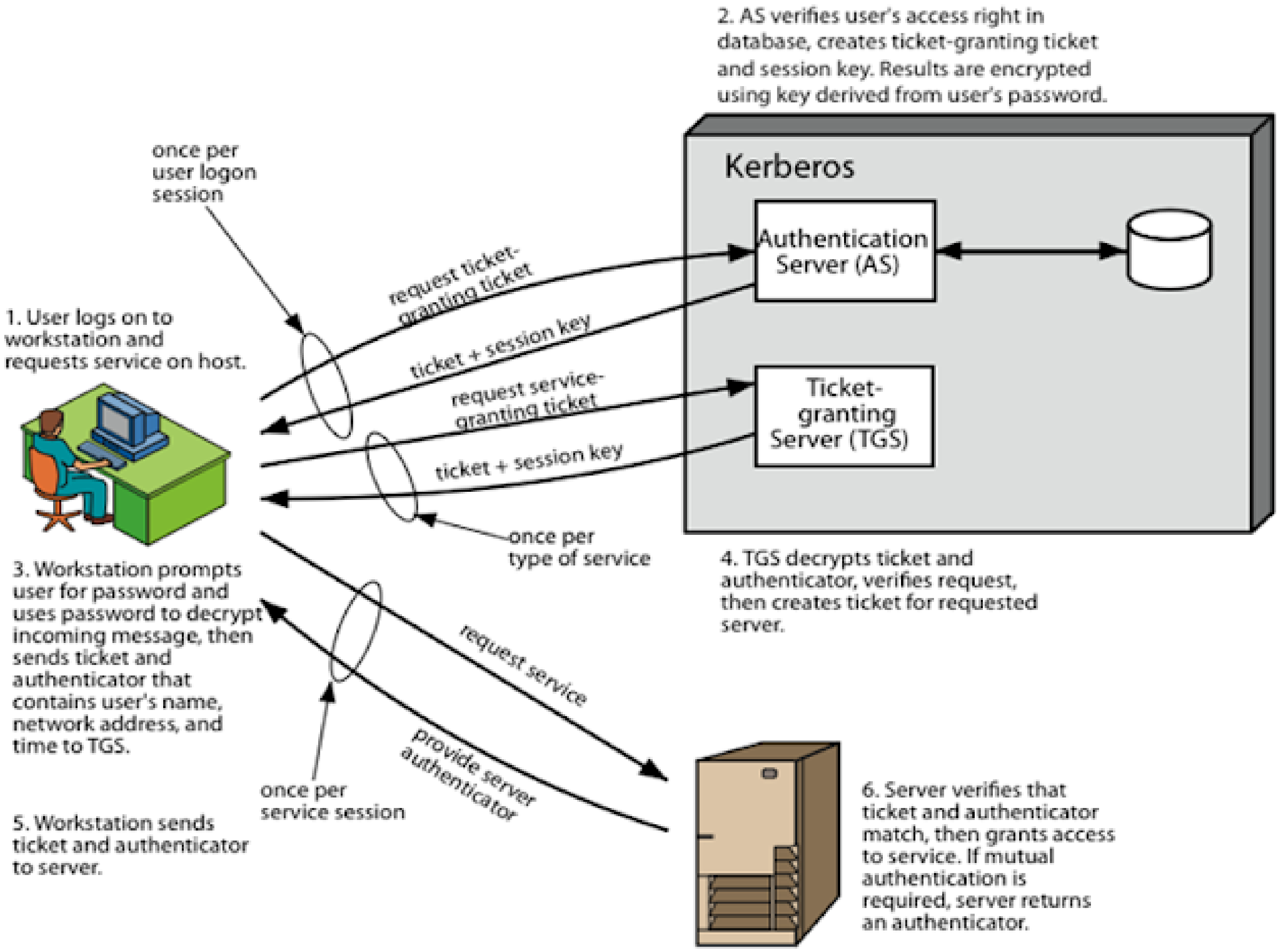


K_{tgs} = key shared only by the AS and the TGS
K_c = key that is derived from user password
K_v = key shared between server and TGS
$K_{c,tgs}$ = session key for C and TGS
$K_{c,v}$ = session key for C and Server

Summery of Kerberos version 4 message exchange scenario

- Kerberos Realm | Inter-realm authentication .

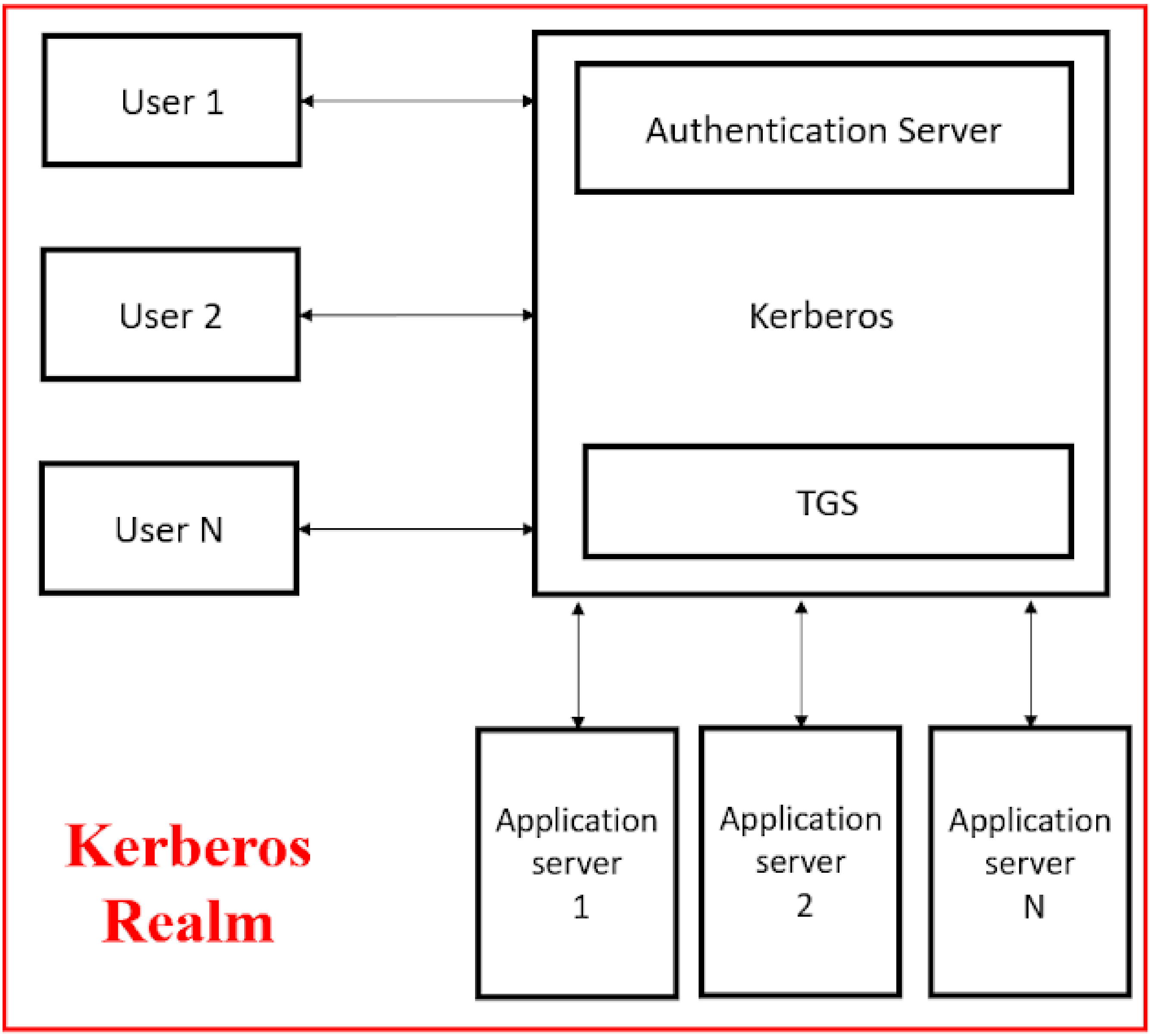
- Kerberios Realm is a Kerberian world that is part of the Kerberians of Kerberia .


2. AS verifies user's access right in database, creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.
Kerberos
Authentication Server (AS)
Ticket-granting Server (TGS)
once per user logon session
1. User logs on to workstation and requests service on host.
request ticket-granting ticket
ticket + session key
request service-granting ticket
ticket + session key
once per type of service
3. Workstation prompts user for password and uses password to decrypt incoming message, then sends ticket and authenticator that contains user's name, network address, and time to TGS.
4. TGS decrypts ticket and authenticator, verifies request, then creates ticket for requested server.
request service
provide server authenticator
once per service session
5. Workstation sends ticket and authenticator to server.
6. Server verifies that ticket and authenticator match, then grants access to service. If mutual authentication is required, server returns an authenticator.

What is Kerberos Realm

- A full-service Kerberos environment consists of a KerberOS server, a number of clients and application servers .

- Such an environment is referred to as a KerBERos realm .


User 1
User 2
User N
Authentication Server
Kerberos
TGS
Application server 1
Application server 2
Application server N
Kerberos Realm