Kerberos

A network authentication protocol

What is Kerberos?

- Kerberos is a network authentication protocol designed to verify the identity of users and entities within a computer network.

- Kerberos issues tickets, allowing access only to authenticated and authorized users or systems.

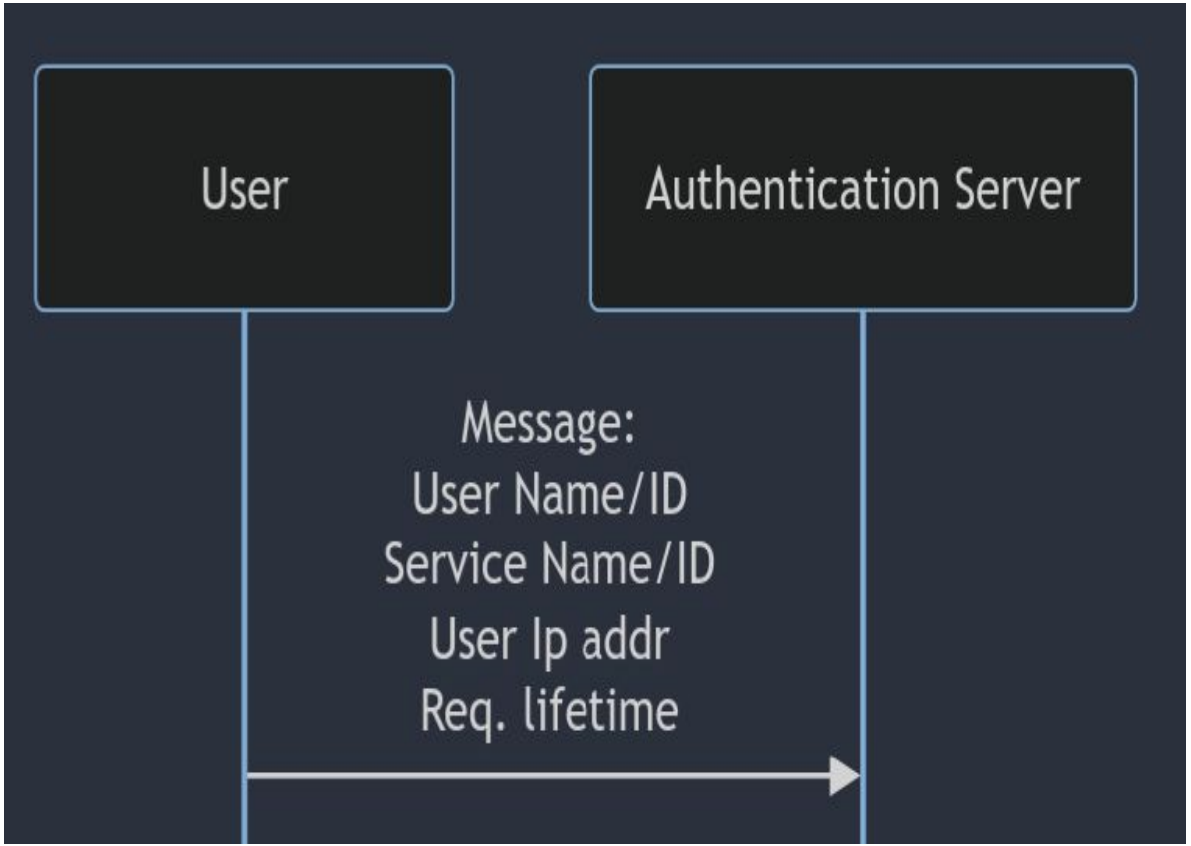
- Kerberos was initially developed at the Massachusetts Institute of Technology (MIT) and has become a standard for secure authentication in various environments.

Core Components

- Kerberos runs as a third-party trusted server known as the Key Distribution Center (KDC)

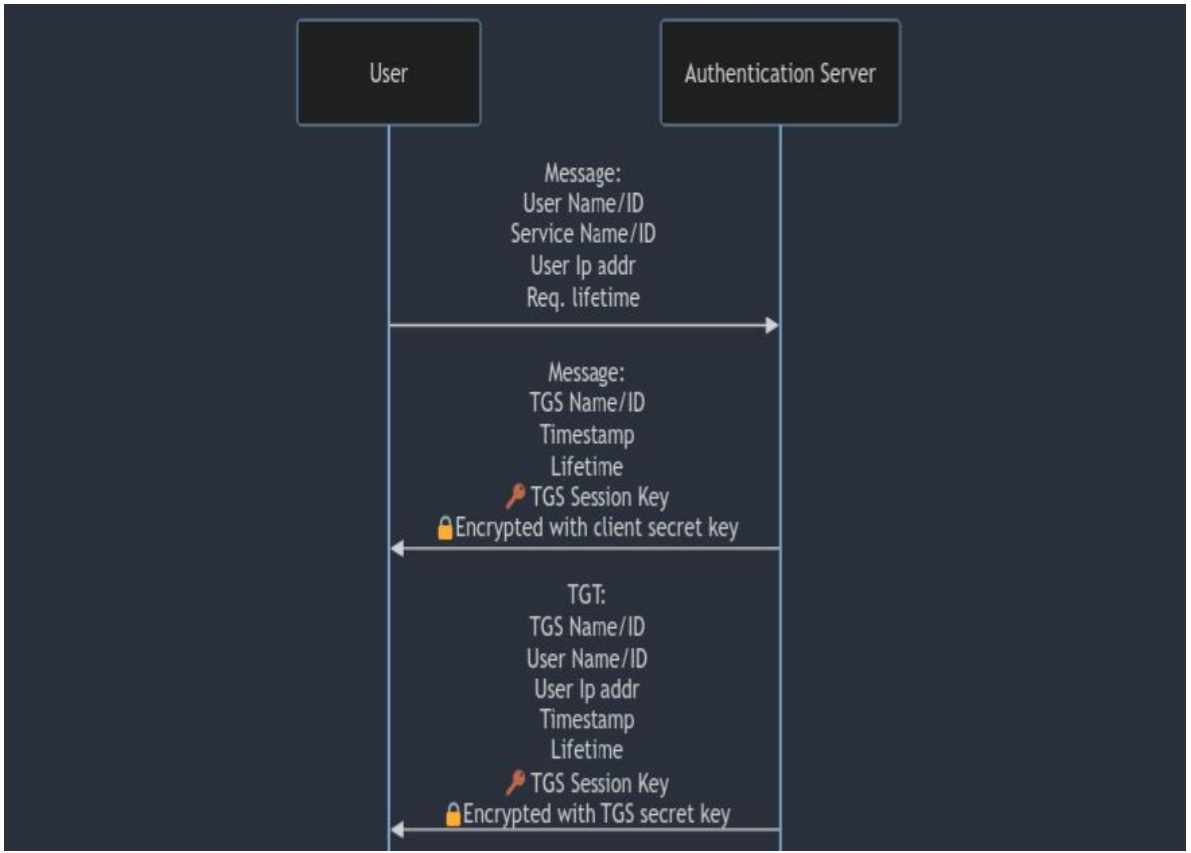
- The KDC has three main components:
  - An authentication server that performs the initial authentication and issues ticket-granting tickets for users.
  - A ticket granting server that issues service tickets that are based on the initial ticket-granting tickets
  - A database of secret keys for all the users and services that it maintains.

How Does Kerberos Work?



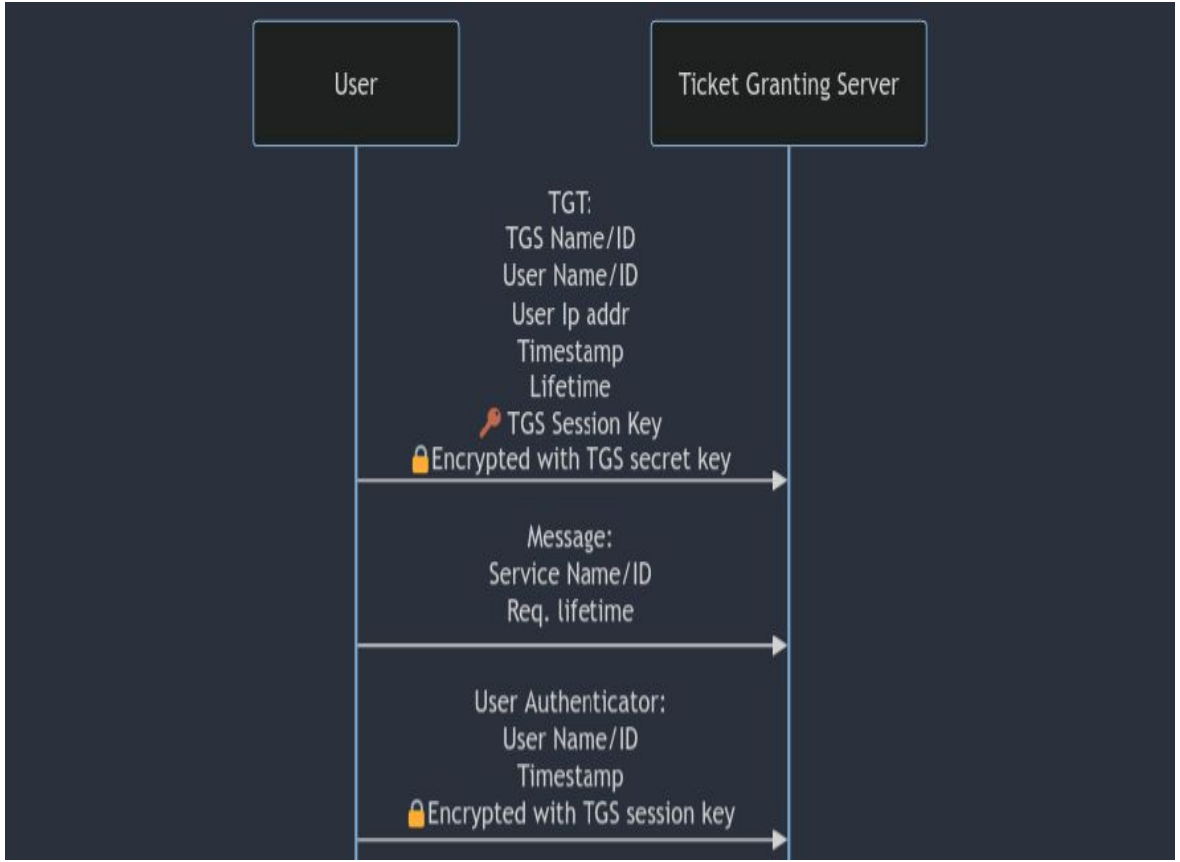
- User sends an unencrypted message containing relevant info to the AS.
- AS stores info about the valid users and their secret key.
- Upon reception the AS checks if the User Name/ID is valid.

How Does Kerberos Work?



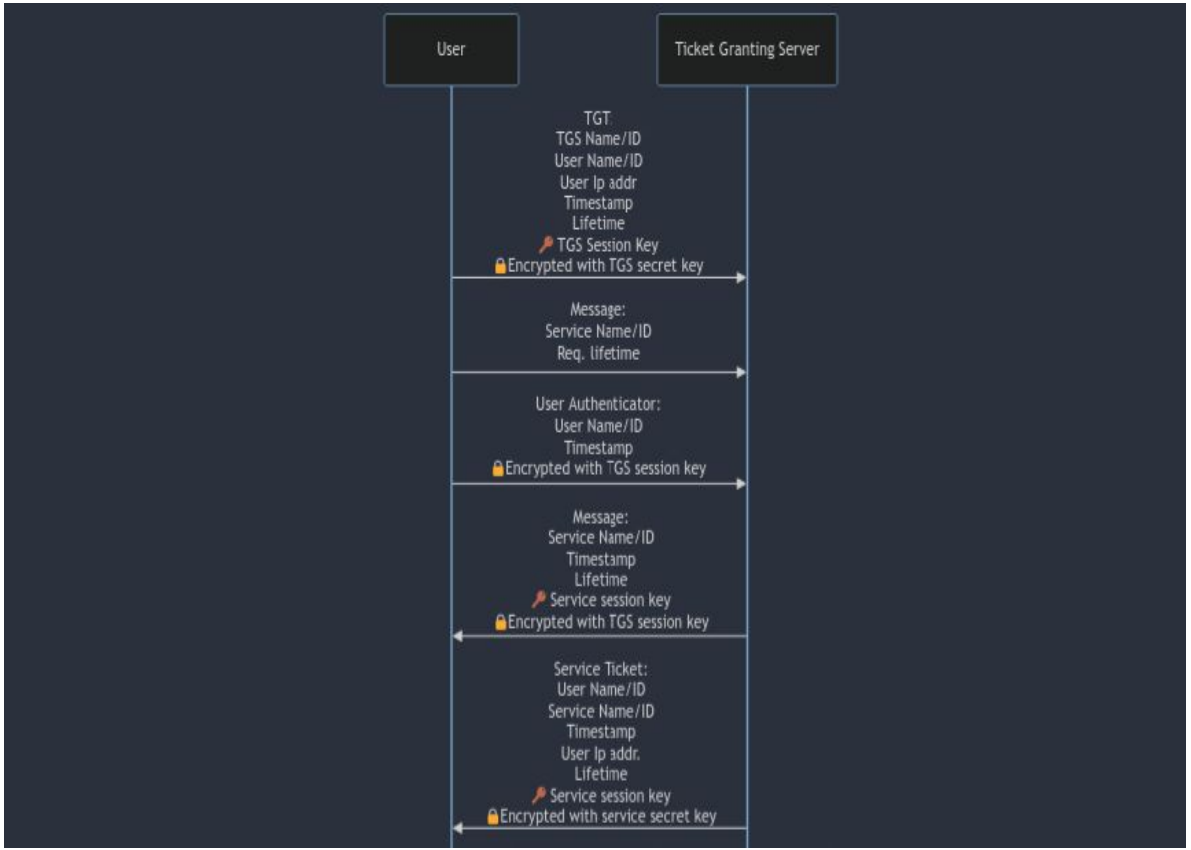
- If the user is valid the AS sends two messages to the user.
- Each message contains a randomly generated symmetric key.
- The first message is encrypted with the user's secret key.
- The second message,the TGT is encrypted with the TGS secret key.

How Does Kerberos Work?



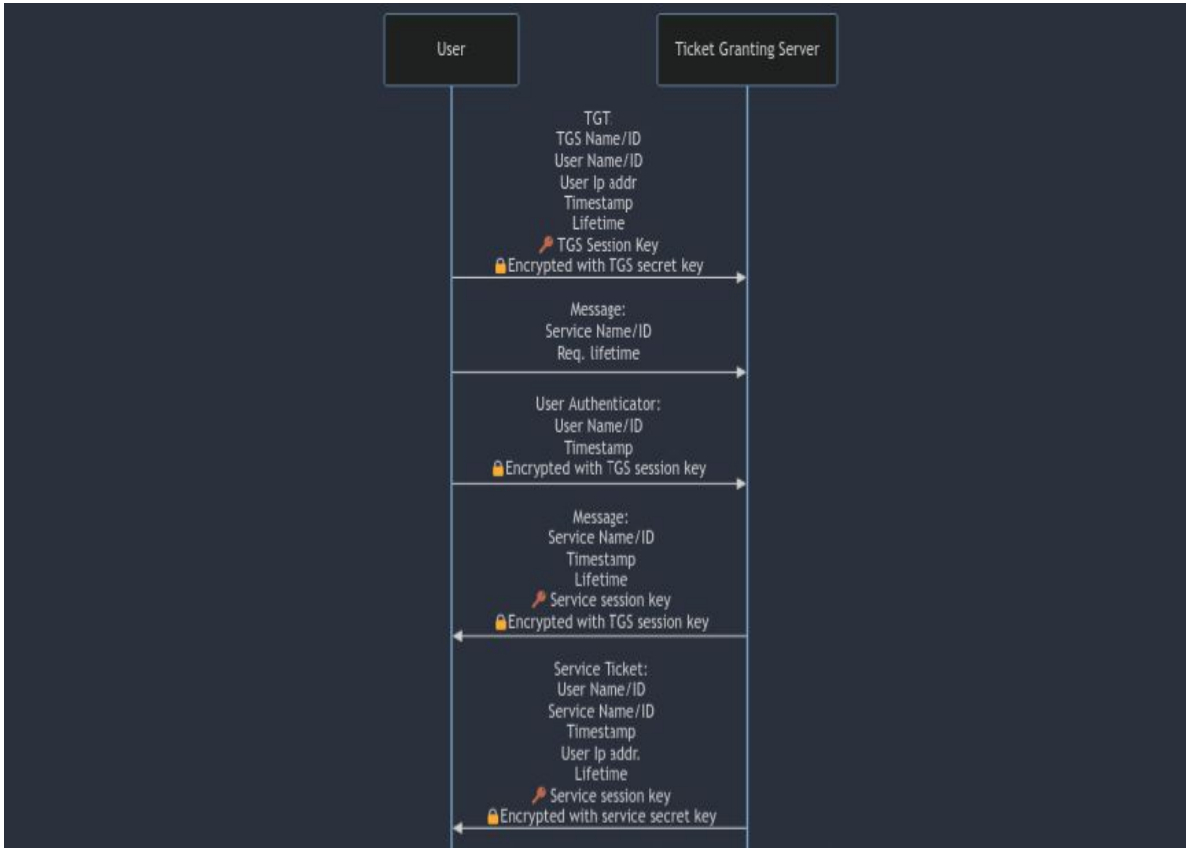
- The user decrypts the first message with his secret key and gets the TGS session key.
- User creates two new messages
  - First message is in plain text containing the service id.
  - Second message is the User authenticator message encrypted with TGS session key.
- Sends these messages to TGS along with the TGT.

How Does Kerberos Work?



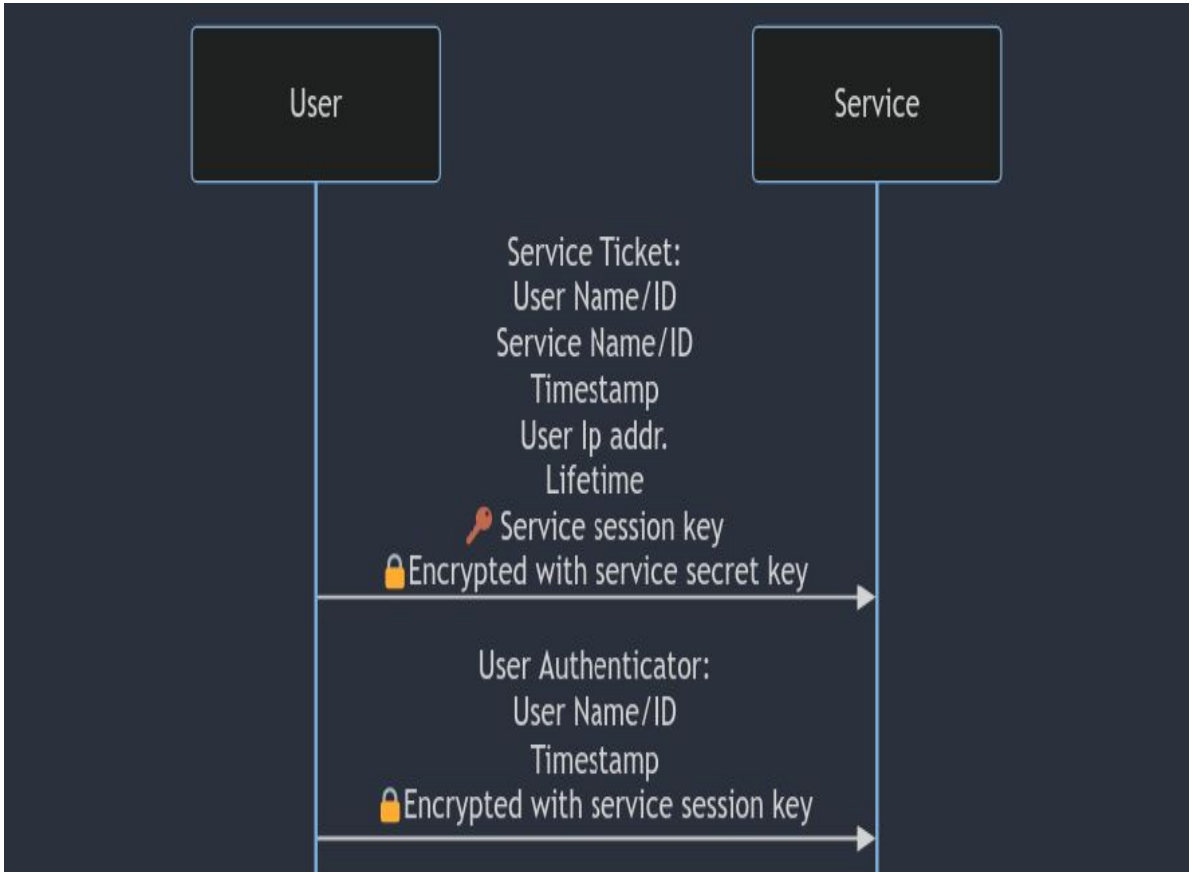
- TGS checks if the Service Name/ID is valid.
- Decrypts TGT and gains access to the TGS session key.
- Uses TGS session key to decrypt User Auth. message.
- Validates data.

How Does Kerberos Work?



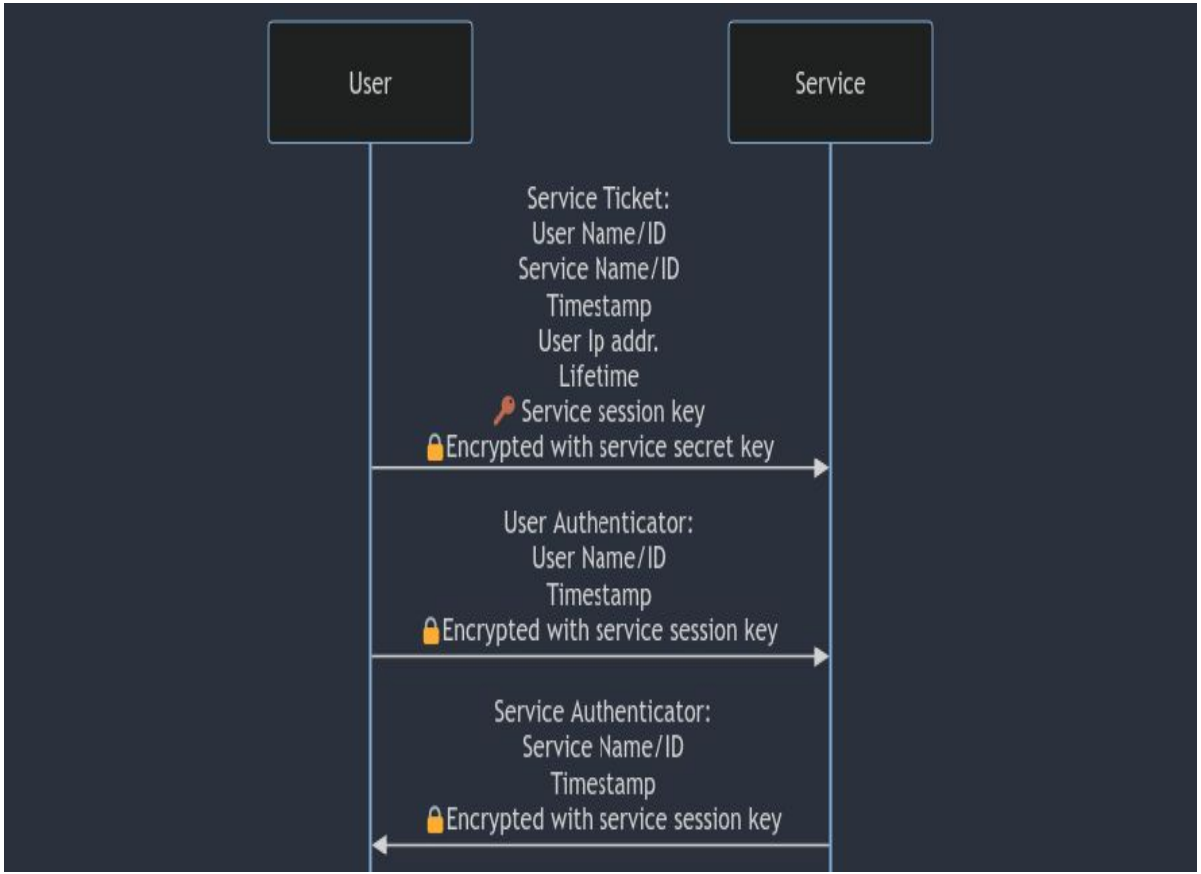
- TGS now creates two messages each containing a randomly generated symmetric key along with other info.
- First message is encrypted with TGS session key.
- Second message, the Service ticket is encrypted with Service secret key.

How Does Kerberos Work?



- User decrypts the first message using the TGS session key and gains access to the service session key.
- Then creates a new User Authenticator message and encrypts it with the service session key.
- Sends this message along with the service ticket to the service.

How Does Kerberos Work?



- The service decrypts the service ticket using it's secret key.
- Uses the session key inside the service ticket to decrypt the user authenticator.
- Does some validation.
- Creates a service authenticator and encrypts it with service session key.
- User decrypts the received service auth. with its service session key.

Advantages

- Kerberos offers centralized and scalable authentication services for secure communication in distributed computing environments

- User passwords are never transmitted over the network in plain text. Instead, they are used to generate keys locally, enhancing password security.

- Kerberos tickets have a limited validity period, reducing the risk of misuse. Once a ticket expires, users need to re-authenticate to obtain a new one.

Thank You