KERBEROS

Network Authentication Protocol

What is Kerberos?

- Kerberos is a network authentication protocol
- Version 5 provides mechanism for mutual authentication between client and server or two servers.
- The Kerberos Key Distribution Center (KDC) uses the domain's Active Directory service database as it's security account database.
- The protocol was initially developed by MIT in the 1980

Characteristics

- It is a stateless protocol
- Based on symmetric key encryption and communication
- Authentication is based on ticketing system

Key Components

- Authentication via Kerberos is done by the **Key Distribution Center (KDC)**
  - **Authentication service (AS):** Authenticates users when they initially attempt to access a service
  - **Ticket granting service (TGS):** Connects a user with the service server (for example, a file server) based on information stored in the database
  - **Kerberos database:** Where the IDs and passwords are stored, often an LDAP server or the Security Account Manager (SAM) database in an Active Directory environment.

Authentication Process

- **Three pairs of Request-Response**
  - AS_REQ **and** AS_REP
  - TGS_REQ **and** TGS_REP
  - AP_REQ **and** AP_REP

Authentication Process

- **AS_REQ**
  - Security Identifier (SID)
  - Name of the requested service (for example, example.cool.hat)
  - User's IP address
  - Desired lifetime of the Ticket Granting Ticket (TGT). The default is 10 hours and can be changed via Group Policy

Authentication Process

- **AS_REP**
  - First Message (Ticket Granting Ticket)
    - Security identifier (SID)
    - TGS ID
    - Timestamp
    - User's IP address
    - TGT lifetime
    - TGT
    - TGS Session key

Authentication Process

- **AS_REP**
  - Second Message
    - TGS ID
    - Timestamp
    - Lifetime
    - TGS Session key

Authentication Process

- **TGS_REQ**
  - First Message
    - TGT
    - Kerberos ID for service
    - Lifetime

Authentication Process

- **TGS_REQ**
  - Second Message (Authenticator)
    - User ID
    - Timestamp
    - TGS Session key

Authentication Process

- **TGS_REP**
  - First Message (Service Ticket)
    - Service ticket
    - User's ID
    - User's IP address
    - Lifetime
    - Service session key

Authentication Process

- **TGS_REP**
  - Second Message
    - User ID
    - Timestamp
    - Lifetime
    - Service Session key

Authentication Process

- **AP_REQ**
  - First Message
    - Service ticket
    - User ID
    - Timestamp
    - IP Address
    - Timestamp
    - Service session key

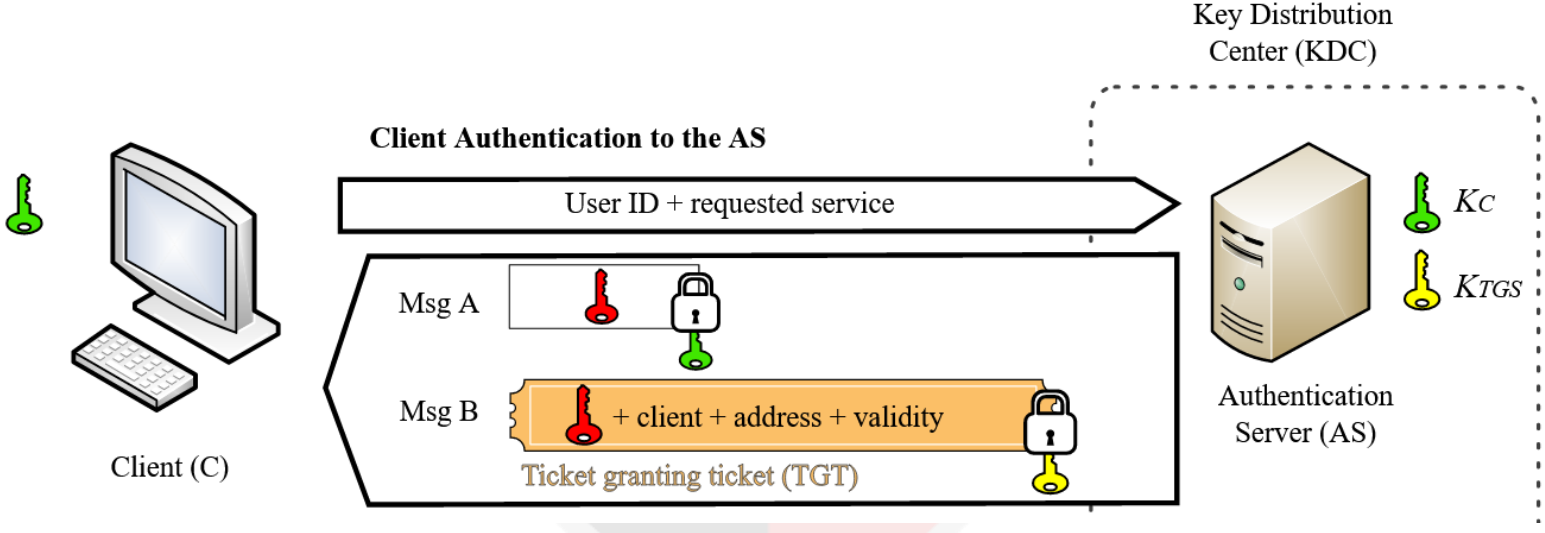
Authentication Process

- **AP_REQ**
  - Second Message (Authenticator)
    - User ID
    - Timestamp
    - Service Session key

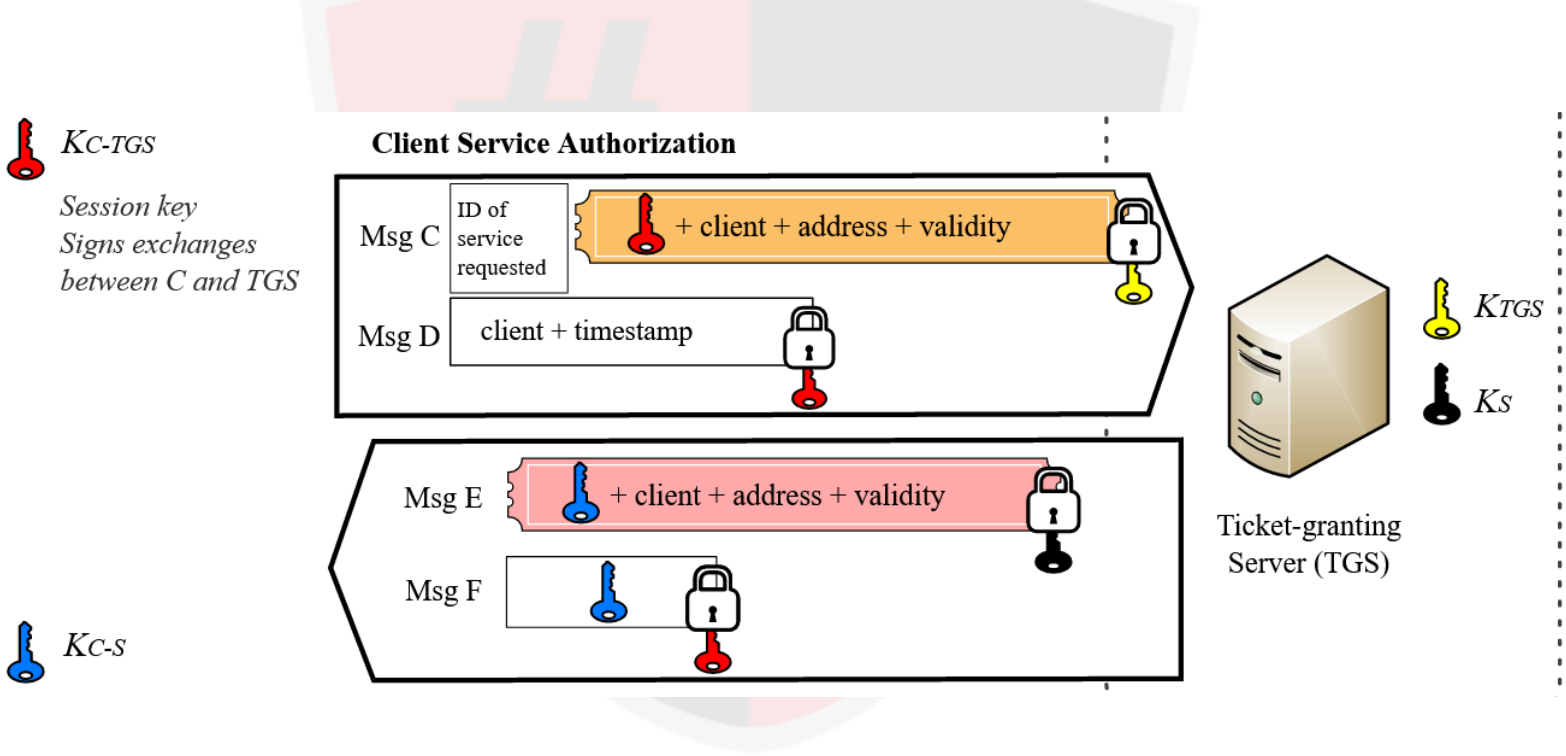
Authentication Process

- **AP_REP**
  - Timestamp
  - Service session key

Authentication Process

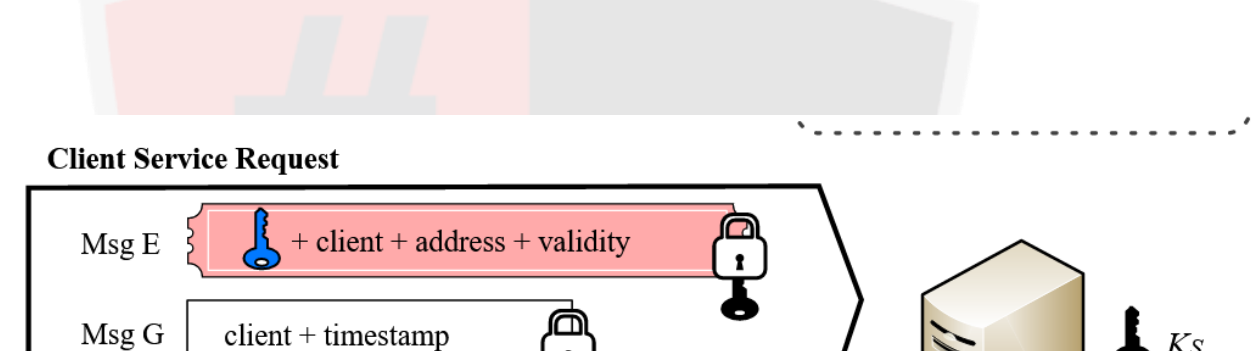


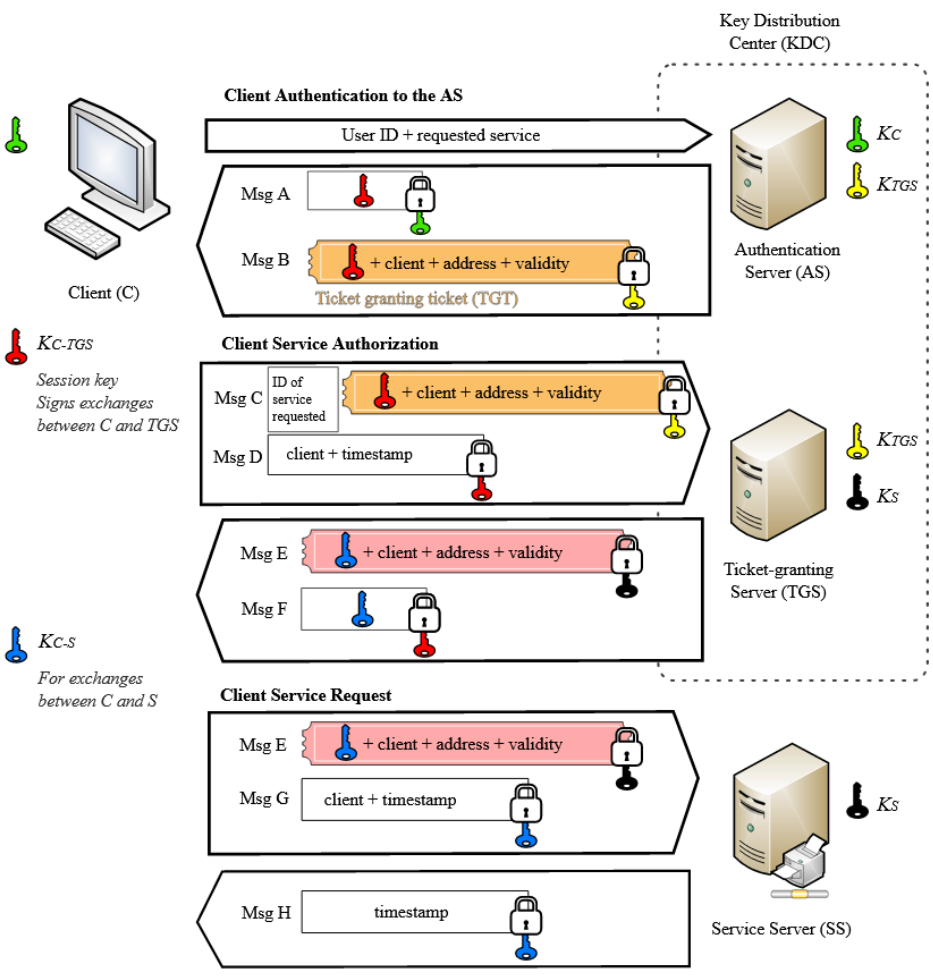
Authentication Process

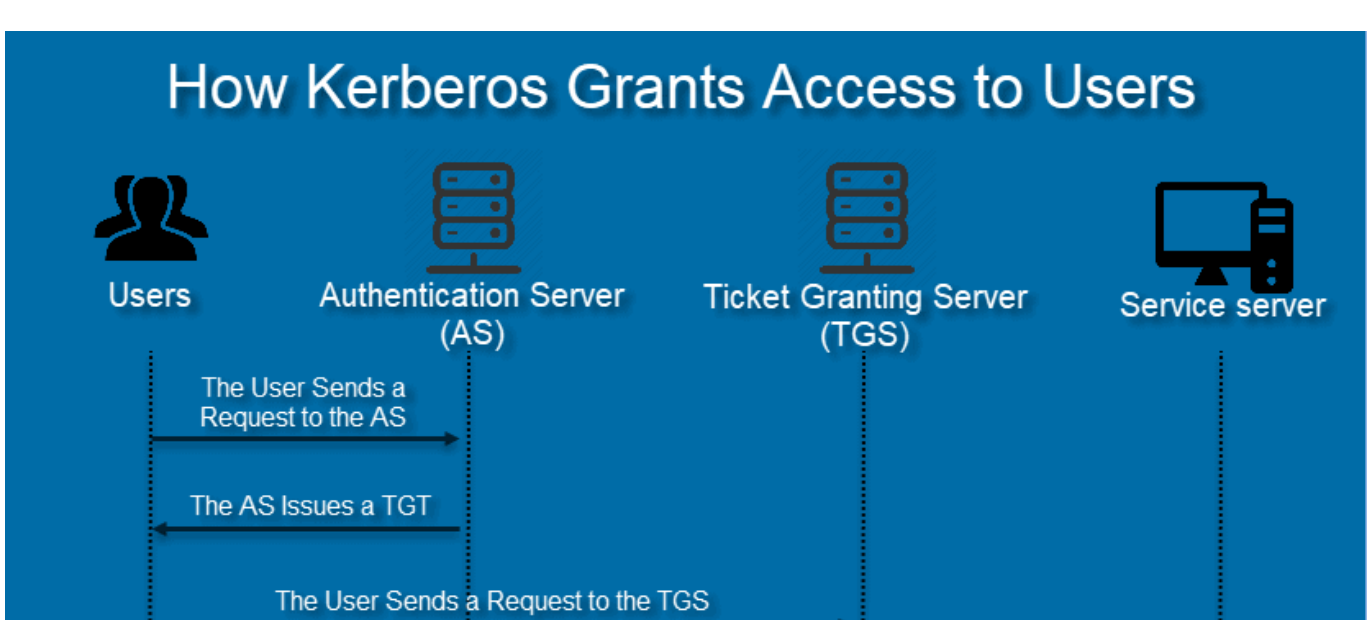


Authentication Process

For exchanges between C and S




Key Distribution Center (KDC)
Client Authentication to the AS
User ID + requested service
Msg A
Msg B
+ client + address + validity
Ticket granting ticket (TGT)
Kc
KTGS
Authentication Server (AS)
Client (C)
Kc-TGS
Session key
Signs exchanges between C and TGS
Client Service Authorization
Msg C
ID of service requested
+ client + address + validity
Msg D
client + timestamp
KTGS
Ks
Ticket-granting Server (TGS)
Msg E
+ client + address + validity
Msg F
Kc-S
For exchanges between C and S
Client Service Request
Msg E
+ client + address + validity
Msg G
client + timestamp
Msg H
timestamp
Ks
Service Server (SS)


How Kerberos Grants Access to Users
Users
Authentication Server (AS)
Ticket Granting Server (TGS)
Service server
The User Sends a Request to the AS
The AS Issues a TGT
The User Sends a Request to the TGS
The TGS Issues a Service Ticket
The User Contacts the File Server with the Service Ticket
The Service Server Grants Access to the User

Features

- Effective Access Control
- Single Sign On
- Limited Lifetime for Key Tickets
- Mutual Authentication
- Reusable Authentication
- Strong and Diverse Security Measures

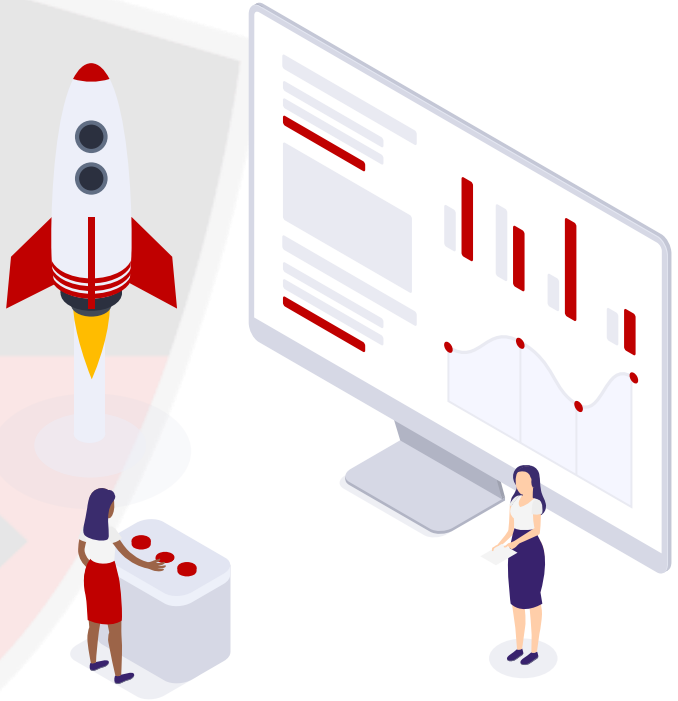
Security Concerns?

- Golden Ticket
- Silver Ticket
- Pass the Hash
- Pass the Ticket
- Overpass the Hash
- Kerberoasting

1

Transition headline

Let’s start with the first set of slides



In two or three columns

Yellow

Is the color of gold, butter and ripe lemons. In the spectrum of visible light, yellow is found between green and orange.

Blue

Is the colour of the clear sky and the deep sea. It is located between violet and green on the optical spectrum.

Red

Is the color of blood, and because of this it has historically been associated with sacrifice, danger and courage.