KERBEROS

Where does it comes from?

- Cerberus, also known as the hound of Hades. It guards the gates of the underworld.

- Kerberos, authentication protocol developed in 1986 by MIT's Project Anthena

- It is still maintained by MIT Kerberos Team

- Stable Version: 5-1.20

Where does it comes from?

- Based on a protocol designed by Roger Needham and Michael Schroeder in 1978

- Which itself is based on the invention of Howard Rosenblum of NSA in 1967

"Nothing is lost, nothing is created, everything is transformed"

\- Antoine Lavoisier

What is it?

- Kerberos is a network authentication protocol that allows users to securely access services over a physically insecure network. (Definition by MIT)

- It uses:
  - SSO (single sign-on)
  - Symmetric Cryptography

Symmetric X Asymmetric

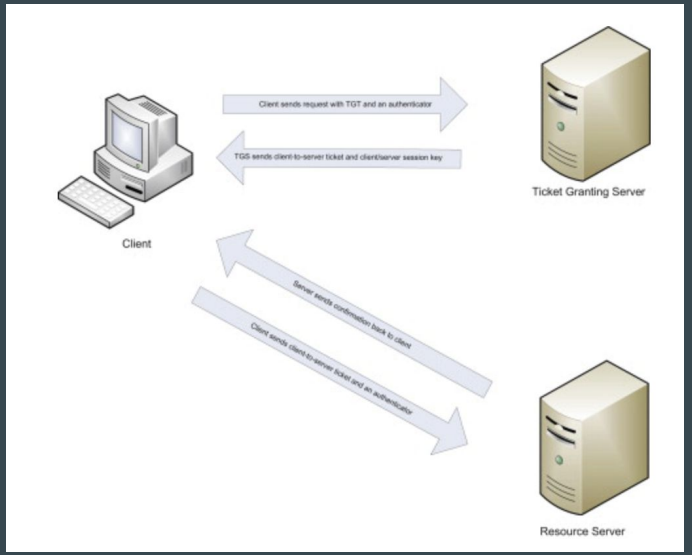
Symmetric Encryption	Asymmetric Encryption
• Symmetric encryption consists of one key for encryption and decryption.	• Asymmetric Encryption consists of two cryptographic keys known as **Public Key** and **Private Key**.
• Symmetric Encryption is a lot quicker compared to the Asymmetric method.	• As Asymmetric Encryption incorporates two separate keys, the process is slowed down considerably.
• RC4 • AES • DES • 3DES • QUAD	• RSA • Diffie-Hellman • ECC • El Gamal • DSA

How does it work?

KDC (Key Distribution Center) Components

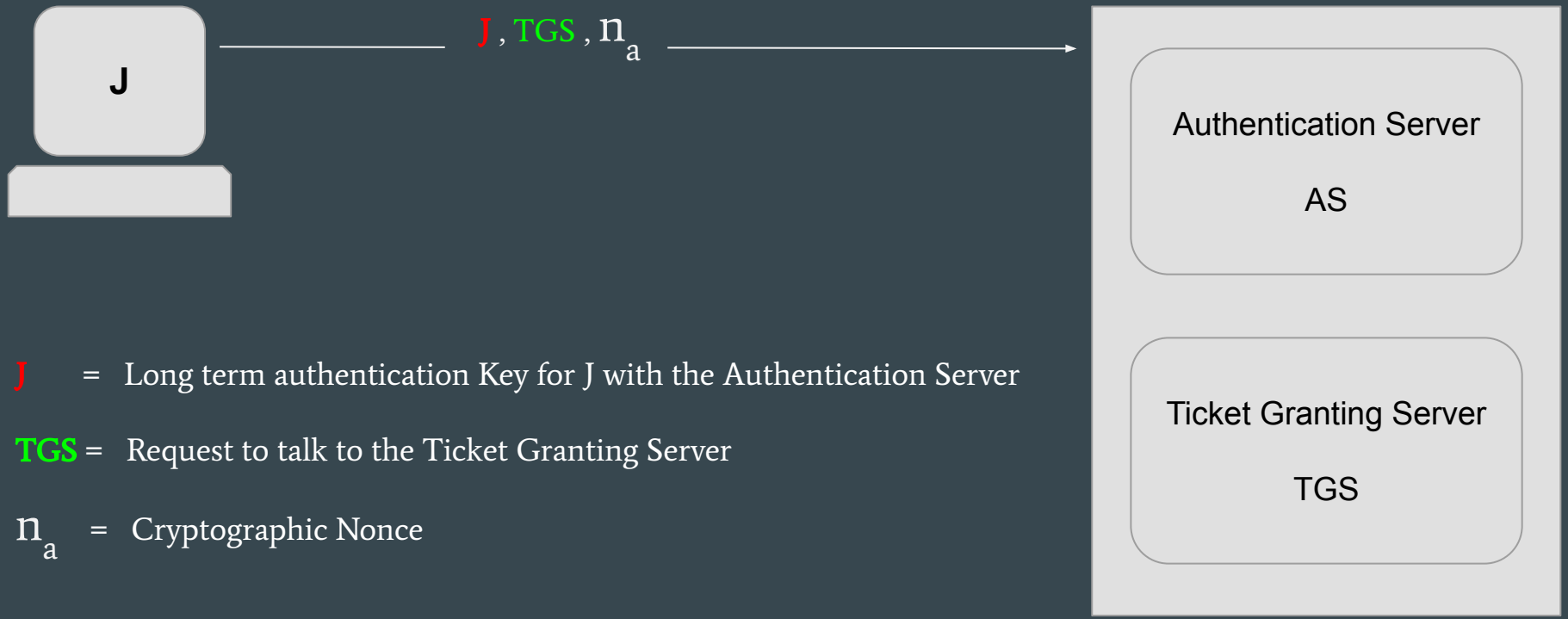
1. Authentication Server

2. Ticket Granting Server



3. Secret Key Database

How does it work?

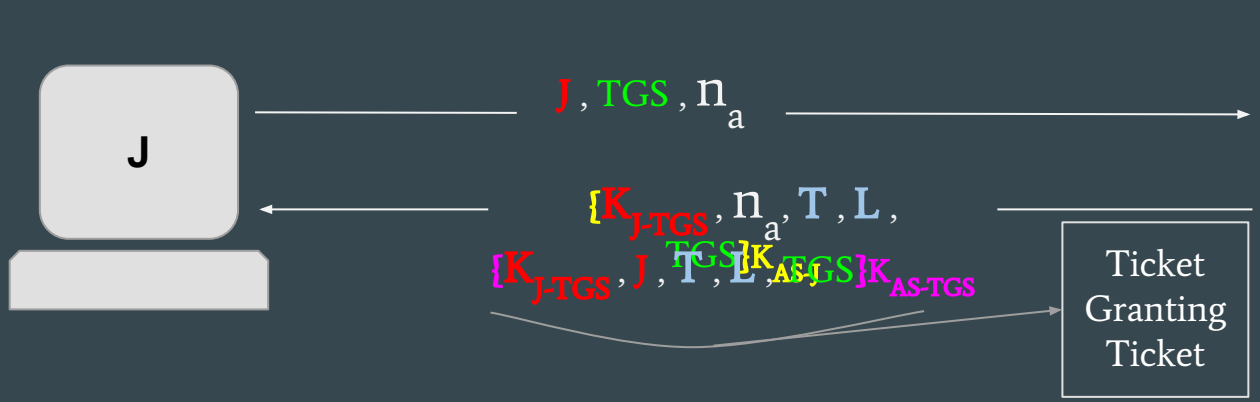


J = Long term authentication Key for J with the Authentication Server

TGS = Request to talk to the Ticket Granting Server

n_a = Cryptographic Nonce

How does it work?



$K_{J\text{-}TGS}$ = Session Key for communication between J and TGS

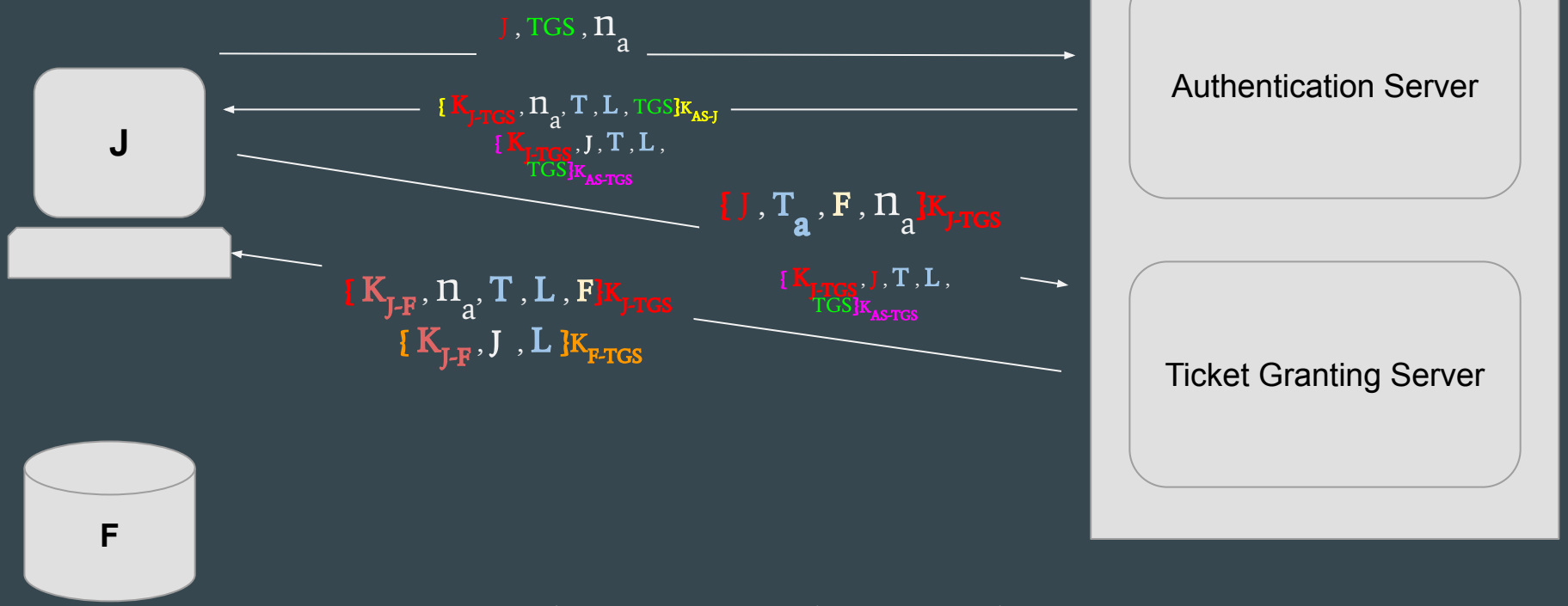
T = Current time

L = Life time of the ticket

$K_{AS\text{-}J}$ = Long Term Key for communication between AS and J

$K_{AS\text{-}TGS}$ = Long Term Key for communication between AS and TGS

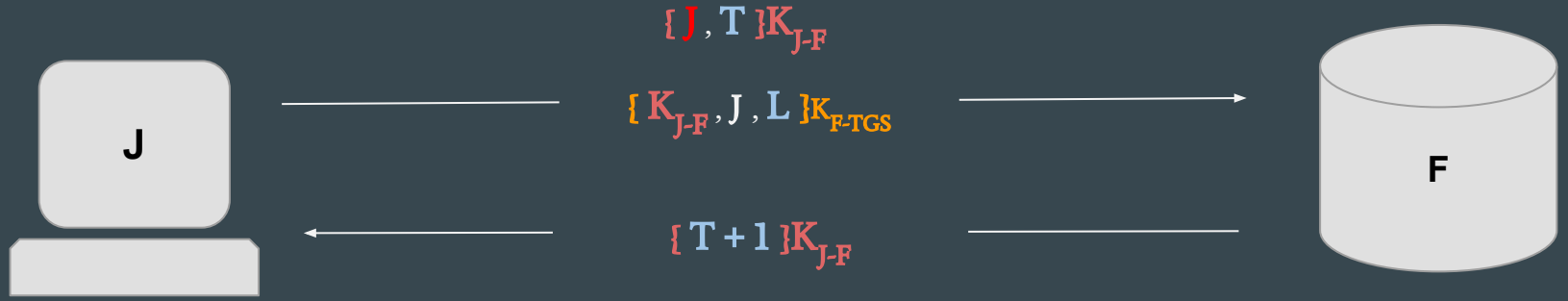
How does it work?



K_{J-F} = Session Key for communication between J and F

K_{F-TGS} = Session Key for communication between F and TGS

How does it work?



Use cases:

- Microsoft's Active Directory
- Apple
- NASA
- Google
- US Department of Defense
- Universities


THANK
YOU!

References

- https://www.kerberos.org/
- https://web.mit.edu/kerberos/
- https://web.mit.edu/kerberos/krb5-latest/doc/
- https://www.youtube.com/watch?v=qW361k3-BtU&t=583s
- https://web.mit.edu/Saltzer/www/publications/Kerberosorigin.pdf
- https://www.ibm.com/docs/en/power8?topic=tasks-manage-kdc