



सी डैक
CDAC



International Conference
on
PKI and Its Applications
(PKIA-2017)
November 14-15, 2017

Hotel Chancery Pavilion, Bangalore



Importance of Session Key in Remote User Authentication

Dr. R. Madhusudhan
Associate Professor



Department of Mathematical and Computational Sciences
National Institute of Technology Karnataka
Srinivasnagar PO, Surathkal,
Mangalore-575025



www.pkiindia.in



www.facebook.com/pkiindia

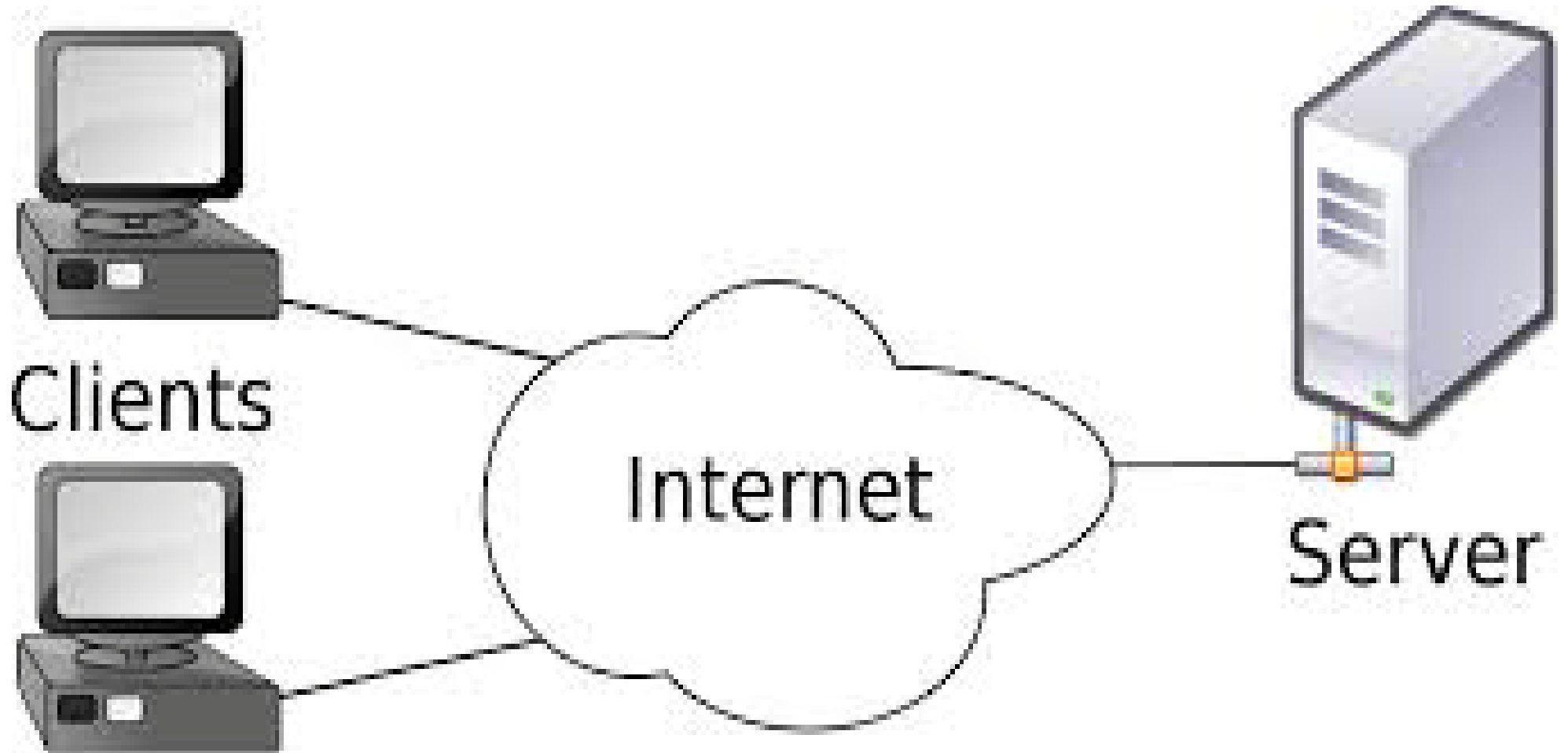


[PKIIndia](https://www.youtube.com/PKIIndia)



[@pkiindia](https://twitter.com/pkiindia)

Client Server Architecture



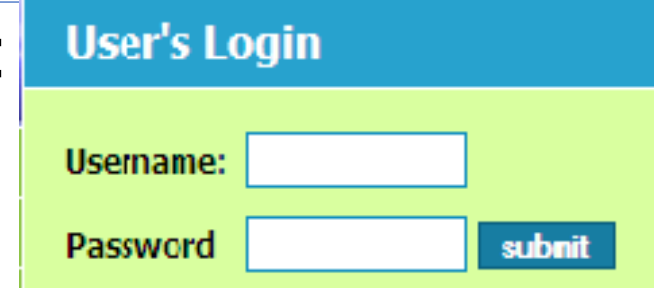
AUTHENTICATION



Authentication Methods

We can authenticate an identity in three ways:

- Something the user knows
Password, PIN etc..



User's Login

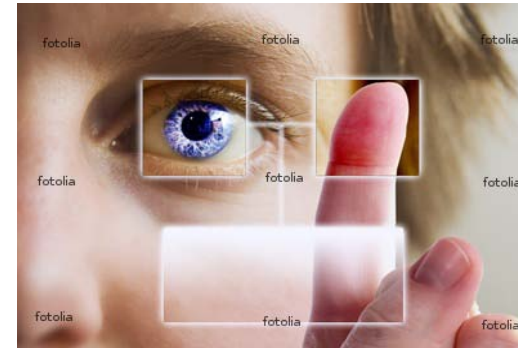
Username:

Password

- Something the user has
Security token,
Credit /debit/smart card,
Mobile phone



- Something the user is
fingerprint, Iris scan,
face, vein etc.. called a biometric



SESSION KEY

- ✓ In the computing world, a session refers to a limited time of communication between two systems.
- ✓ Some sessions involve a client and a server, while other sessions involve two personal computers.
- ✓ A session key is a single-use symmetric key used for encrypting all messages in one communication session.
- ✓ They are created to exist for a very short time.



Thank You



Thank You Thank You