# IT Security and Security compliance in Industry

Manish Arya

# Outline

- Introduction
- What is information security
- Basic techniques of information security
- Pre Shared Key (PSK)
- Public key infrastructure (PKI)
- Compliance in industry
- Security Standards compliance
- Regulatory compliance
- Q&A

# Introduction

- Data
- Information
- Data and Information Security

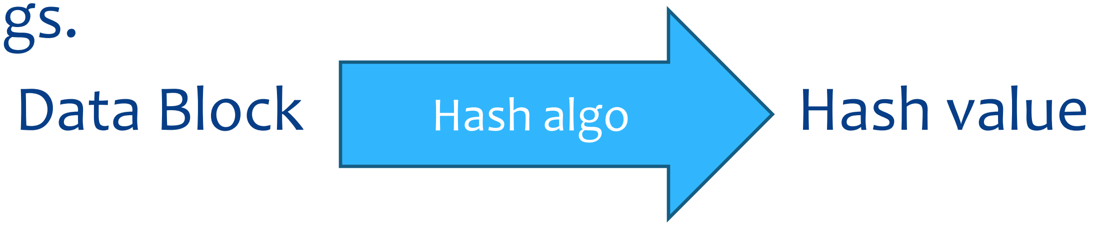
# Information Security

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. Information security covers confidentiality, integrity and availability of data in all forms.

# Core of information security

- Hash (checksum)
- Encryption
- PSK and PKI
- Digital signature
- Digital certificates

- **Hash values** are generated by one way algorithms generating collision resistant and fix length output strings.

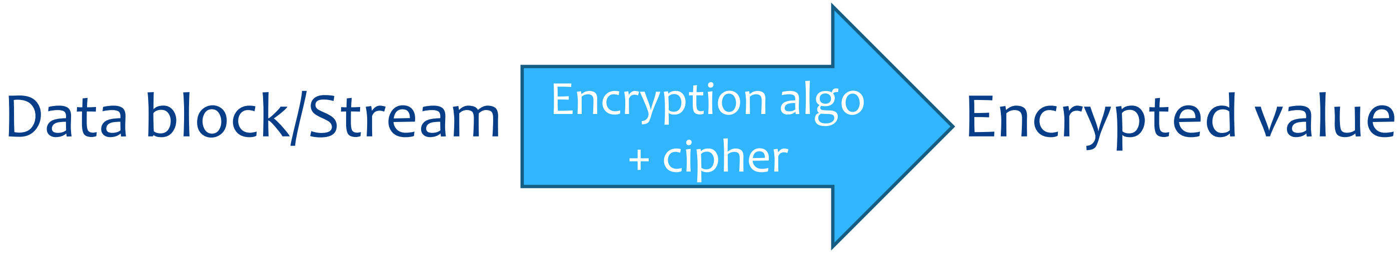


Data Block

Hash algo

Hash value

- **Encryption** is just scrambled form of data block or stream, which is usually done in combination of a cipher key.



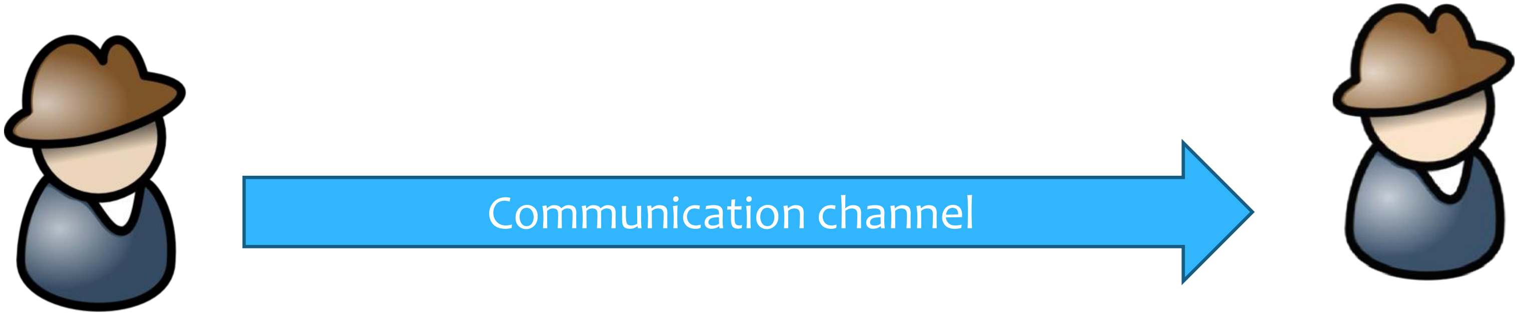
Data block/Stream

Encryption algo + cipher

Encrypted value

- Common encryption algorithms: Crypt, DES, 3DES, AES.
- Common Hash algorithms: SHA-1, SHA-2, MD5.

# PSK (pre shared key) security mechanism



Communication channel

encrypt(Message + cipher key)

decrypt(Message + cipher key )

Cipher key is shared  between systems/users to encrypt and decrypt messages sent over public communication channels

# Applications of PSK mechanism

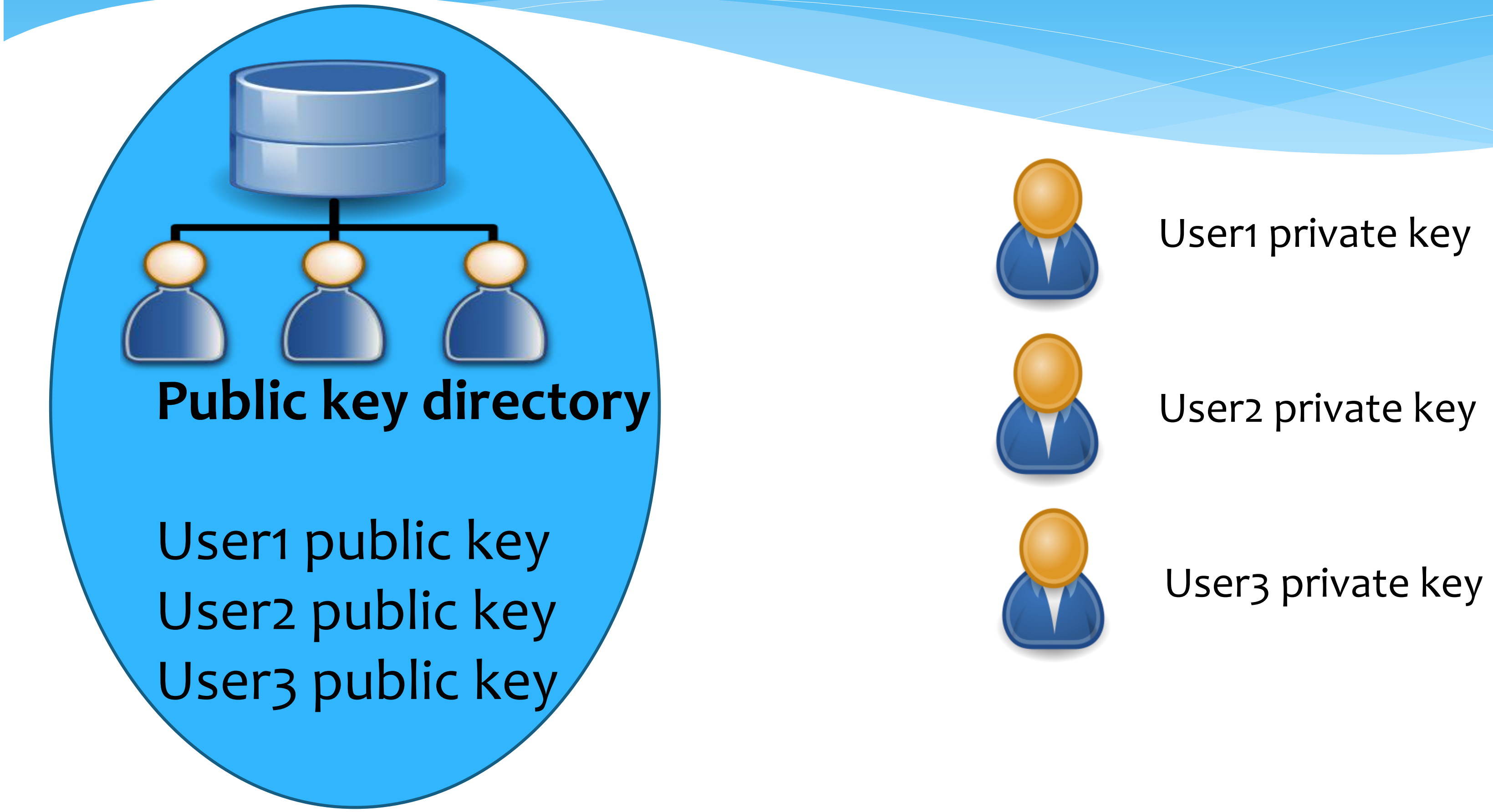
- Exchange encrypted messages.

- Authentication by using combination of PSK and hashing methods.

# Public key infrastructure (PKI)

- PKI is preferred to overcome shortfall of sharing common cipher key amongst various systems and risk of compromising the common key.
- PKI mechanism works with key pair of public and private keys.

# Public key infrastructure (PKI)



**Public key directory**

User1 public key
User2 public key
User3 public key

User1 private key

User2 private key

User3 private key

pgp.mit.edu, keyserver.pgp.com

# Key pair generation

```
ssh-keygen -t {dsa|rsa}
```

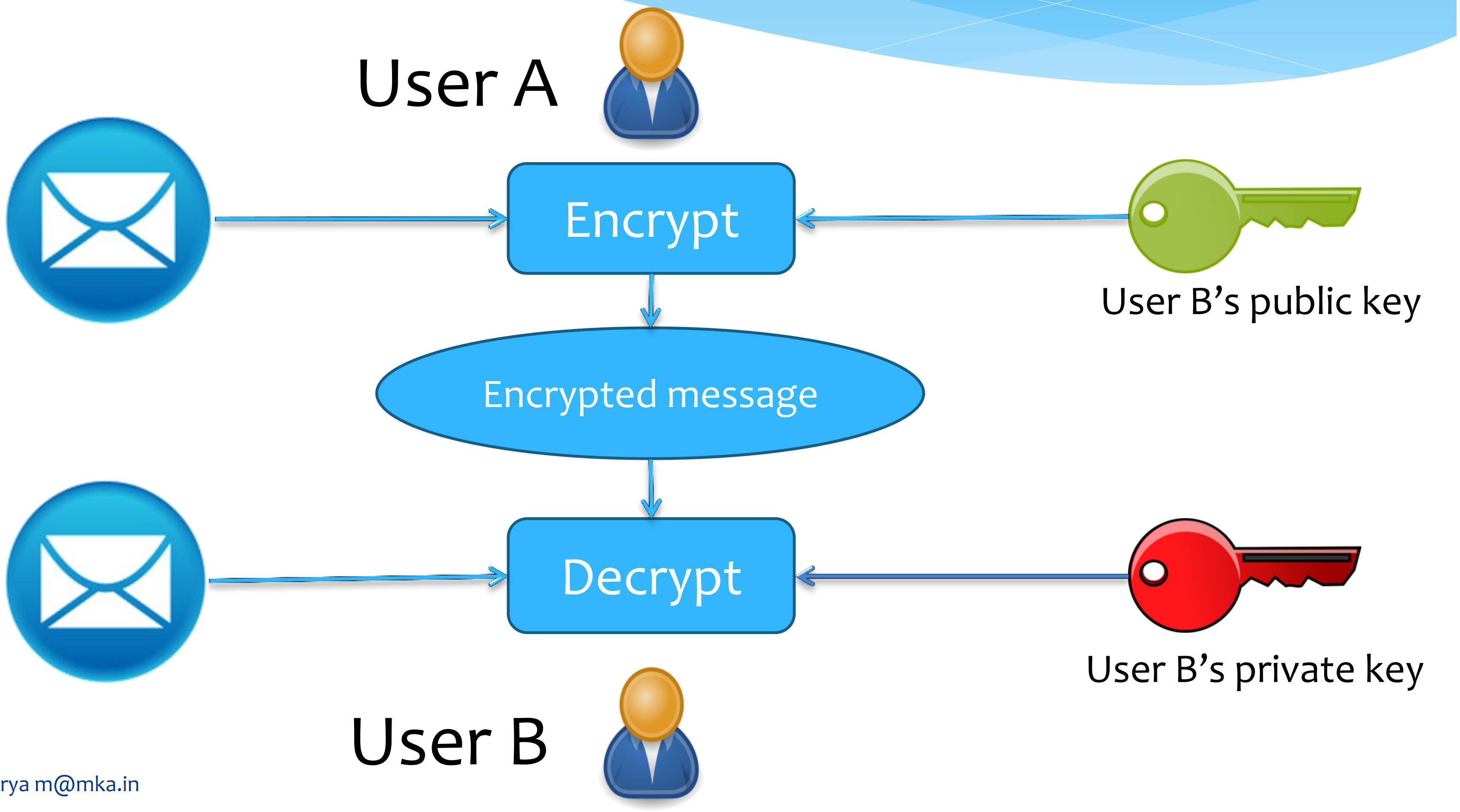
You can mention DSA or RSA algorithms and it will also prompt for optional passphrase key. This key will act as password of your private key.

```
-rw------- 1 root root  668 Mar 16 11:54 id_dsa
-rw-r--r-- 1 root root  616 Mar 16 11:54 id_dsa.pub
```

# Applications of PKI

- Encrypt messages
- Digital signing
- SSL certificates

# ‘A’ sending encrypted message to ‘B’



User A

Encrypt

User B’s public key

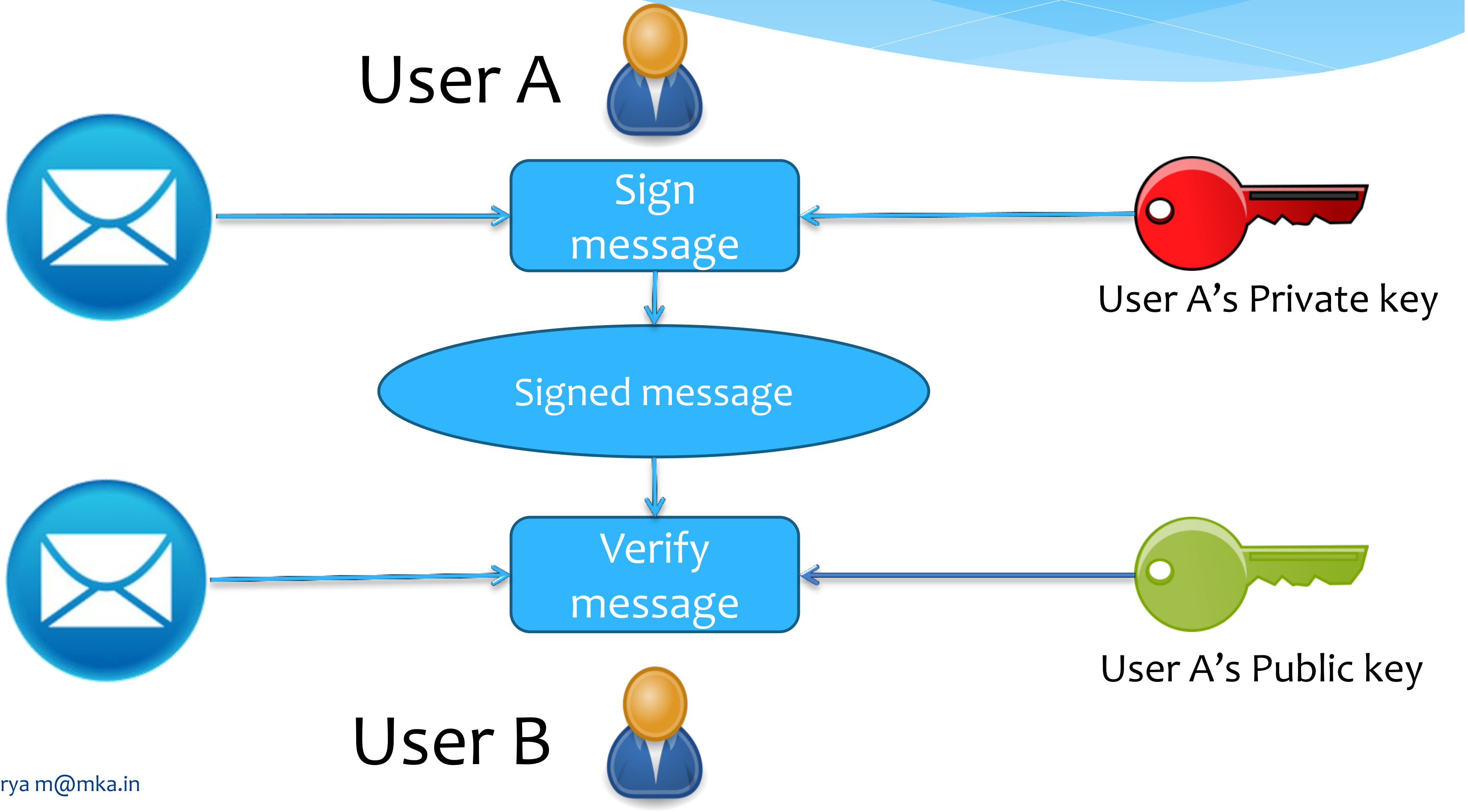
Encrypted message

Decrypt

User B’s private key

User B

# ‘A’ sending signed message to ‘B’



User A

Sign message

User A’s Private key

Signed message

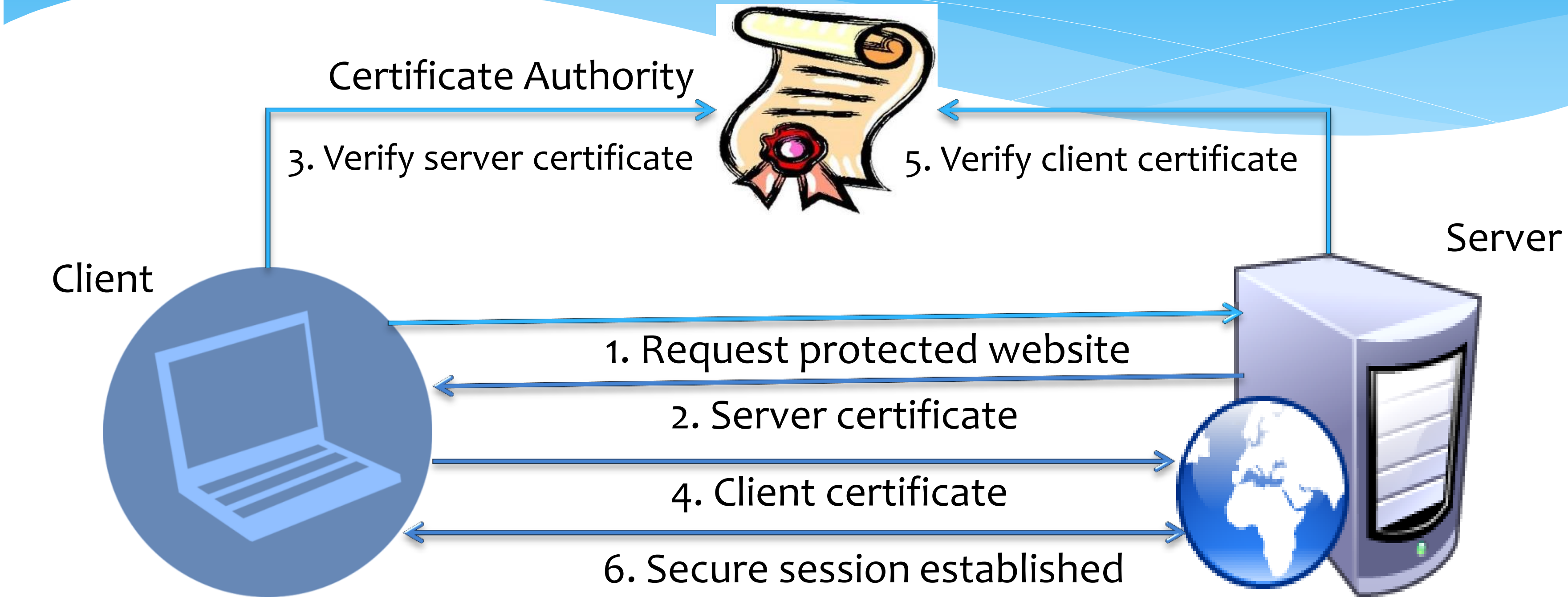
Verify message

User A’s Public key

User B

Manish Arya m@mka.in

# SSL certificate



Certificate Authority

3. Verify server certificate

5. Verify client certificate

Client

Server

1. Request protected website

2. Server certificate

4. Client certificate

6. Secure session established

Client certificate store

Server certificate store

# Security Compliance

Broadly security compliance in industry covers

- Authorized access to IT systems and data.
- Availability of services and data to legitimate users/systems.
- Information/Data protection.
- Data integrity.
- Identify and address potential threats, vulnerabilities, and risks.

# Security Standards compliance

- There are several global security standards, some are generic and some are specific to the nature of industry.
- ISO127001 most widely adopted and accepted generic standard across organizations.
- Payment Card Industry Data Security Standard (PCI-DSS).
- HIPAA or the Health Insurance Portability and Accountability Act.

# Coverage of security standards

- Perimeter security (premises).
- Physical area access control.
- IT resources protection and access control.
- Host/Device level security (OS hardening)
- Network security (firewall, proxy)

# Benefits IT security certification

- Provides customers and stakeholders with confidence in how you manage risk.
- Helping getting new business retaining existing customers.
- Manages and minimizes risk exposure.
- Builds security awareness amongst employees.
- Helps you to comply with other regulations.

# Regulatory compliance covers

**Data retention:** keep traces of activities performed on devices, laptops, mobiles, computers for certain period of time.

**Data protection:** Data gathered in retention process have to be secure from authorized access, modification, deletion.

**Data privacy:** defines what data can or cannot be retained. For eg some parts personal information of an individual can be prohibited from retention.

# Regional regulatory compliance

- UK – ofcom
- India – Telecom Regulatory Authority of India
- USA – Federal Communications Commission, SOX

# Regulatory compliance is must !

- No direct visible business benefit.
- If a organization wants to do business in a geography then it must adhere to the norms laid down by regional regulatory and legal bodies.
- Any non-compliance can lead to cancelation of operator license and regulatory may impose heavy penalties.
- Regulatory/legal compliance is also important for National security and prevent potential large scale frauds.

Q&A

# Thanks!