Dr. B. R. Ambedkar National Institute of Technology

PUBLIC KEY INFRASTRUCTURE

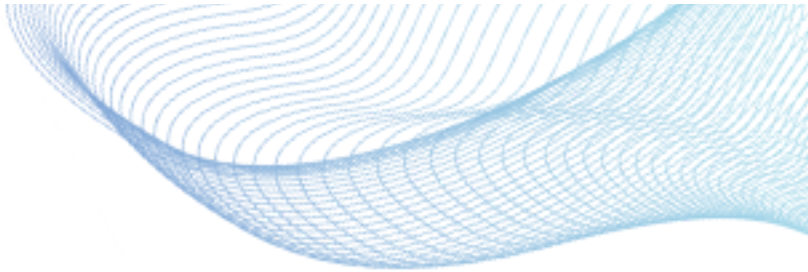
Presented By:

1. Sanket Sudhir Kolte
2. Shreedhar Gangwar
3. Abhinav Bains
4. Sushant Singh

Presented To:

Dr Kunwar Pal

TABLE OF CONTENT



INTRODUCTION TO PKI

Public Key Infrastructure (PKI) is a system of digital certificates, Certificate Authorities, and other security mechanisms that enable secure and trusted communication over the internet. PKI is the foundation for many critical security applications, including secure web browsing, email encryption, and digital signatures.

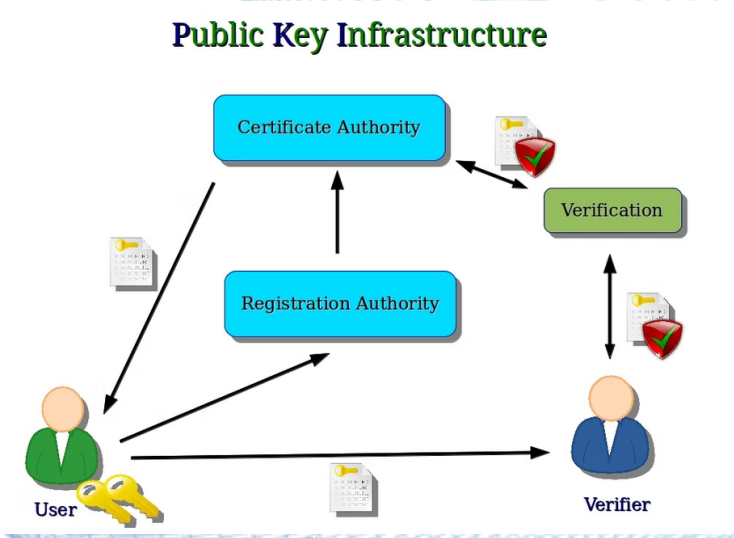


Figure 1

PRINCIPLES OF PKI:

Confidentiality, Integrity, and Authentication

Confidentiality

PKI ensures that sensitive information is only accessible to authorized parties through the use of encryption.

Integrity

PKI guarantees that data has not been tampered with or altered during transmission.

Authentication

PKI verifies the identities of the parties involved in a digital transaction, preventing impersonation

KEY COMPONENTS OF PKI

Certification Authorities

CAs are trusted entities that issue and manage digital certificates, providing the trust anchor for the PKI system.

Registration Authorities

RAs verify the identities of entities requesting certificates and pass this information to the CA.

Repositories & Relying Parties

Repositories store and distribute certificates, while relying parties use the certificates to verify identities and encrypt/decrypt data.

PKI DUTIES AND SERVICES

Certificate Management:

- PKIX is based on X.509, it needs to handle all duties related to certificates.
- Issuing certificates to users/entities.
- Renewing certificates before expiration.
- Revoking certificates if compromised or no longer needed.

Key Management:

- Secure storage of private keys.
- Regular updates of keys as needed.

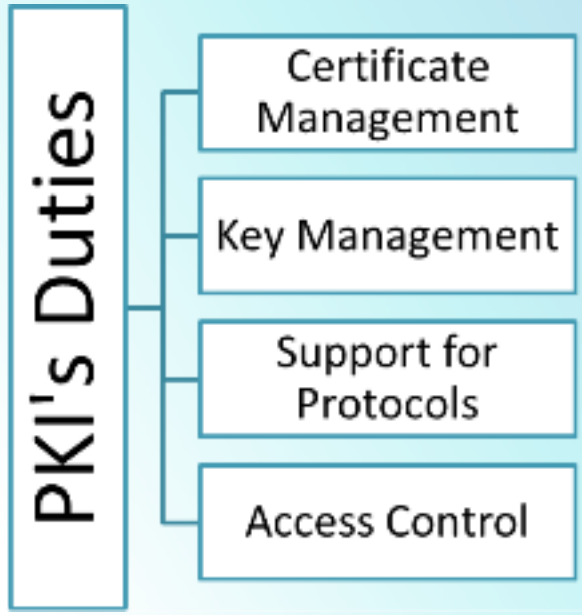


Figure 2

PKI DUTIES AND SERVICES (CONT'D)

Support for Protocols:

- PKI enables secure communication over the Internet by providing certificates for SSL/TLS encryption and authentication.
- PKI supports IPSec VPNs (Virtual Private Networks) for encrypted and authenticated IP-based communication between network devices.

Access Control:

- PKI databases containing certificate and key information are protected against unauthorized access.
- Role-based access control (RBAC) ensures that only authorized personnel can manage and administer PKI components.

TRUST MODELS IN PKI

There should be many CAs, each responsible for creating, storing, issuing, and revoking a limited number of certificates. The trust model defines rules that specify how a user can verify a certificate received from a CA. There three trust model as below

- Hierarchical Model
- Mesh Model
- Web of Trust

HIERARCHICAL MODEL

In this model, there is a tree-type structure with a root CA. The root CA has a self-signed, self-issued certificate; it needs to be trusted by other CAs and users for the system to work.

In the given figure shows a trust model of this kind with three hierarchical levels. The number of levels can be more than three in a real situation.

The figure shows that the CA (the root) has signed certificates for CA1, CA2, and CA3; CA1 has signed certificates for User1, User2, and User3; and so on. PKI uses the following notation to mean the certificate issued by authority X for entity Y.

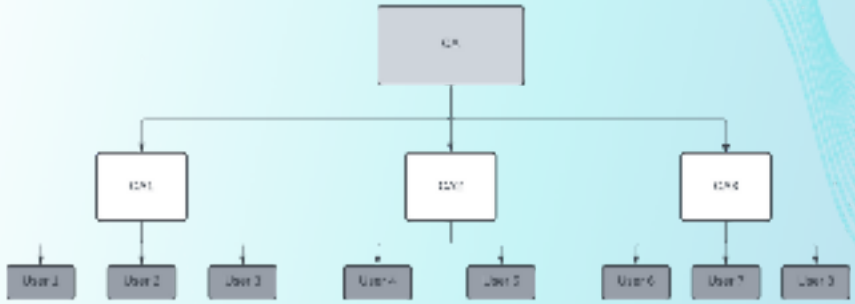


Figure 3

Mesh Model

The hierarchical model may work for an organization or a small community. A larger community may need several hierarchical structures connected together. One method is to use a mesh model to connect the roots together. In this model, each root is connected to every other root, as shown in Figure.

Figure shows that the mesh structure connects only roots together; each root has its own hierarchical structure, shown by a triangle. The certifications between the roots are cross-certificates; each root certifies all other roots, which means there are N (N − 1) certificates. In Figure 15.21, there are 4 nodes, so we need 4 × 3 = 12 certificates. Note that each double-arrow line represents two certificates.

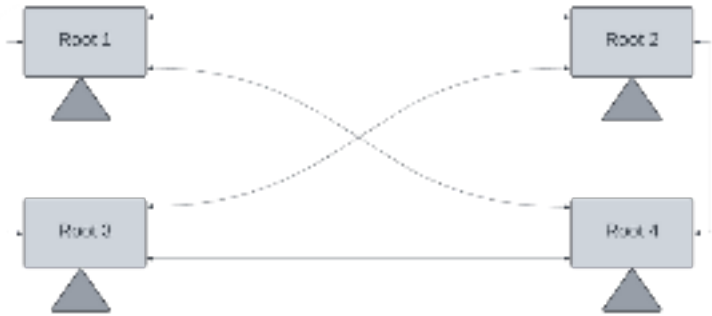


Figure 4

WEB OF TRUST

Definition :

The Web of Trust, used in PGP, is a decentralized model for secure communication. Users validate each other's keys directly, creating a network of trust without centralized authorities. It enables independent identity verification and secure communication, suitable for personal and small-scale contexts.

Application:

- PGP uses the Web of Trust model to verify the authenticity of public keys and establish secure email communication channels.
- Some decentralized file sharing networks incorporate Web of Trust mechanisms to establish trust between peers sharing content.

Advantage:

Decentralized nature reduces reliance on centralized authorities prone to single points of failure.

Challenges:

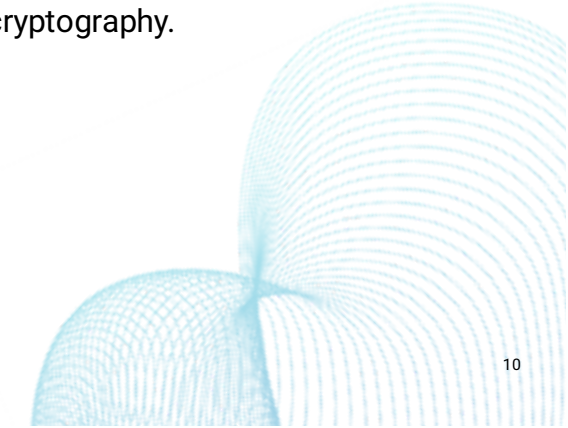
- Subjective nature of trust levels can lead to inconsistencies and potential security risks.
- Requires active community participation and ongoing maintenance of trust relationships.

COMPARISON OF PKI WITH SYMMETRIC KEY CRYPTOGRAPHY

PKI:
PKI uses asymmetric (public-key) cryptography, where each entity has a public and private key pair.

Symmetric Key:
Symmetric key cryptography uses a shared secret key between communicating parties, requiring secure key exchange.

Advantages:
PKI provides better scalability, key management, and non-repudiation compared to symmetric key cryptography.



PKI IMPLEMENTATION CHALLENGES AND CONSIDERATIONS

1 Certificate Lifecycle Management

Effectively managing the issuance, renewal, and revocation of certificates is crucial for PKI success.

2 Trust and Scalability

Building a trusted PKI ecosystem and ensuring it can scale to support a large number of users and certificates.

3 Interoperability

Ensuring PKI systems can seamlessly integrate with other security technologies and applications.

4 User Adoption

Encouraging end-users to properly manage and utilize their digital certificates and PKI features.

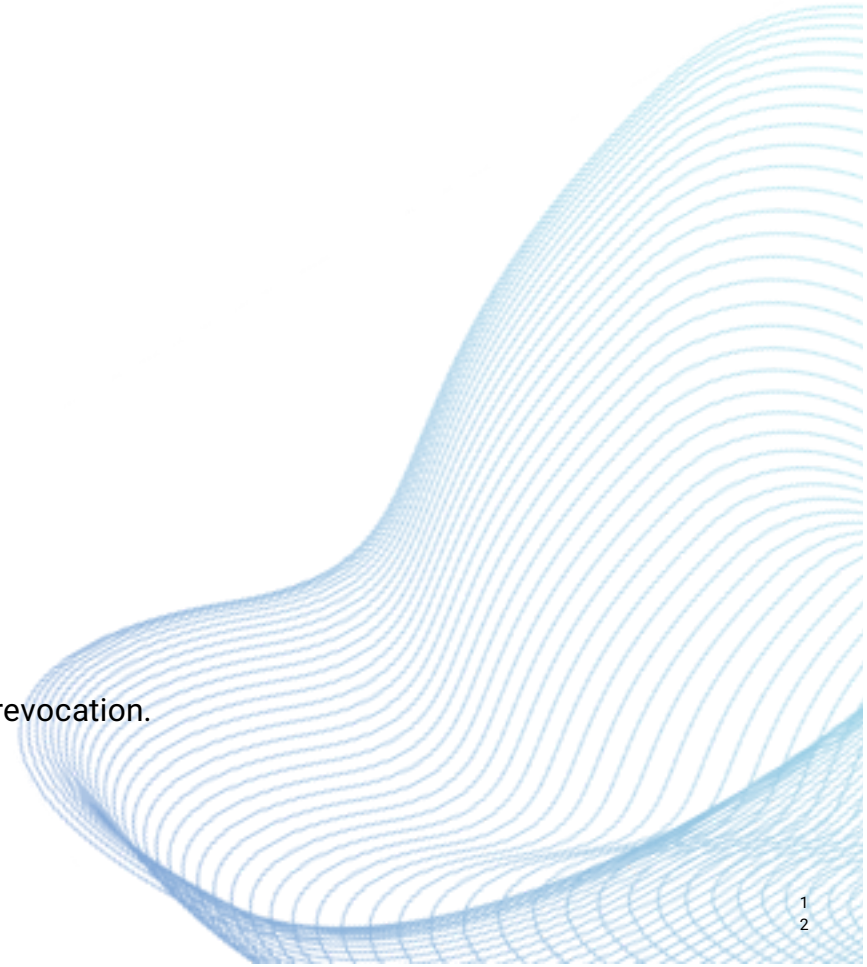
PKI IMPLEMENTATION EXAMPLES

Real-World Use Cases:

- Government agencies for secure document signing.
- Healthcare organizations for patient data protection.
- Financial institutions for secure transactions.

Challenges

- Scalability issues with large PKI deployments.
- Interoperability between different PKI systems.
- Security considerations for key management and certificate revocation.



Conclusion

Summary:

- PKI is essential for ensuring secure digital communication and authentication.

Importance of PKI:

- Safeguards against cyber threats and supports trust in online transactions.

THANK YOU