

Prepared by Dr. Mohammed Anbar

Network Security CYB 603
Overview of Public Key Infrastructure (PKI)

Lecture 7



Learning Objectives

- Explain digital signature ,
- Explain digital certificates,
- Understand Public Key Infrastructure (PKI) and its components,
- Explain the functions and standards of PKI,
- Explain the protocols that rely on PKI standards.

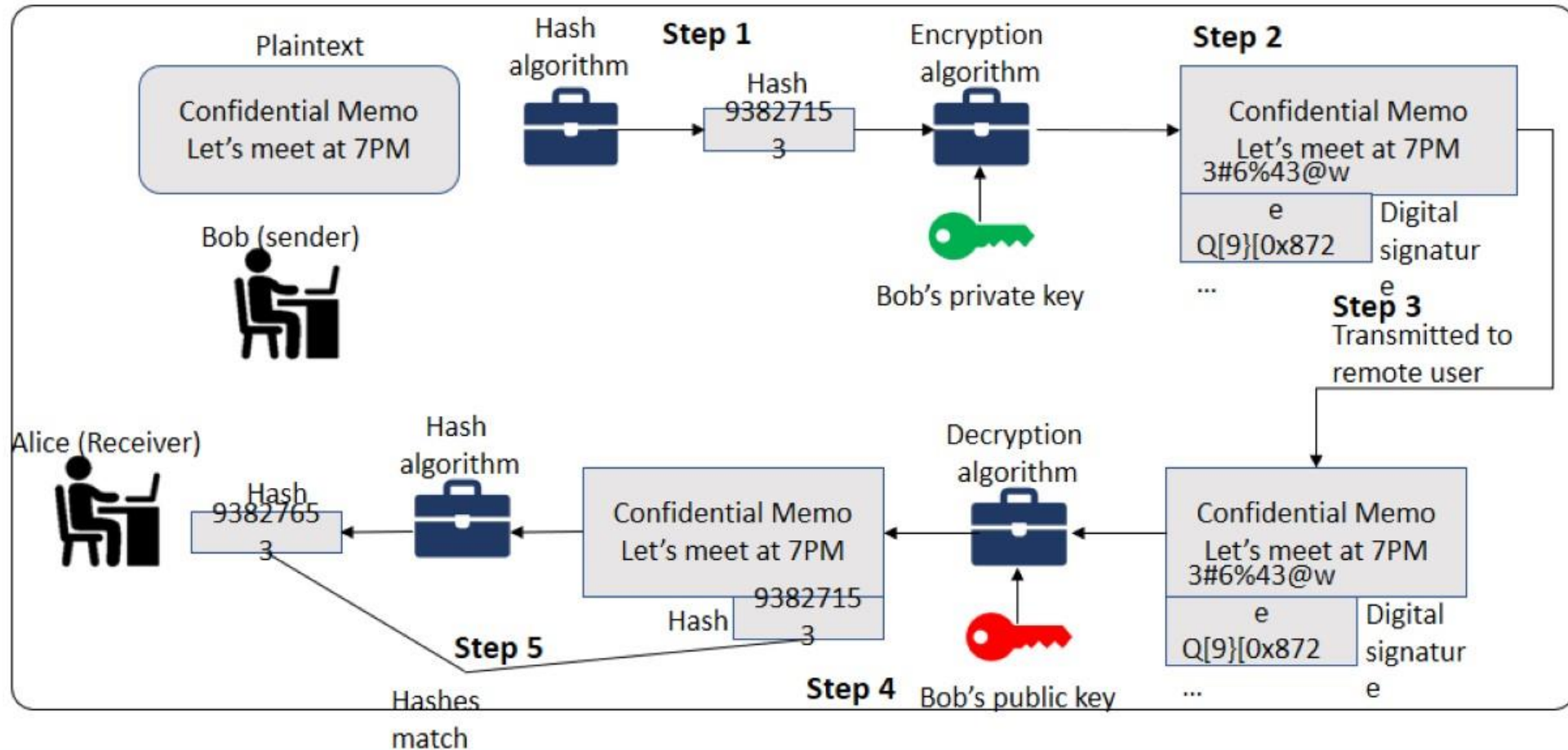
Recap : Public key cryptography

- Public key cryptography uses pairs of keys: a public key that is widely available, and a different private key known only to the person, application, or service that owns the keys.
- The public key can be transmitted unencrypted over insecure lines, since it is not a secret, while the private key must be kept secret.
- The sender's private key may be used to produce a digital signature, an encrypted block of data that, when decrypted by the recipient, verifies the sender's identity (nonrepudiation) as well as the integrity of the data.

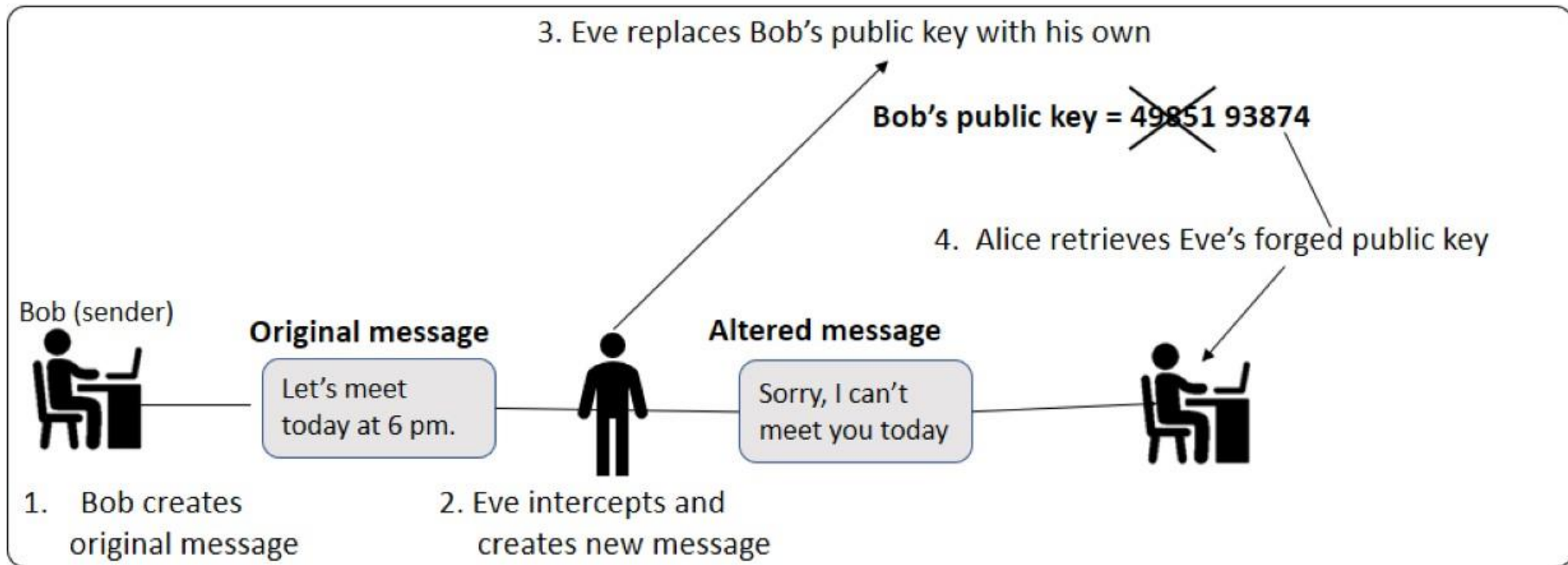
- A digital signature is an electronic signature used to verify the identity of the sender/ signer of a message and to ensure the correctness and validity of information in electronic transactions.
- The use of recognized digital signatures can fulfil requirements of confidentiality, identity authentication, non-repudiation, and integrity of information.
- Digital signatures create a virtual fingerprint that is unique to a person or entity and are used to identify users and protect the information in digital messages or documents.

Chapter 06

Digital Signature Process



- Digital signatures require a reliable way to get public keys
- A forged public key could be used to forge a digital signature



- **Problem #1:** How to distribute Public Keys?
- **Problem #2:** How to know that a particular public key belongs to a certain entity?

- PKI is a set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.
- The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking, and confidential email.
- It is required for activities where simple passwords are an insufficient authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

- PKI involves
 - Public-key cryptography standards
 - Trust models
 - Key management
- PKI is digital certificate management

- Digital certificates can be used to associate or “bind” a user’s identity to a public key
- Digital certificates make it possible for Alice to verify Bob’s claim that the key belongs to him
- When Bob sends a message to Alice, he does not ask her to retrieve his public key from a central site. Instead, Bob attaches the digital certificate to the message

- Bind a user's identity to a public key
- Encrypt channels to provide secure communication between clients and servers
- Encrypt messages to secure Internet e-mail communication
- Verify the identity of clients and servers on the Web
- Verify the source and integrity of signed executable code

- A digital certificate typically contains the following information:
 - Owner's name or alias
 - Owner's public key
 - Name of the issuer
 - Digital signature of the issuer
 - Serial number of the digital certificate
 - Expiration date of the public key

For Alice and Bob to use asymmetric cryptography:

- Alice and Bob must generate public and private keys
- A Certificate Authority (CA) or Registration Authority (RA) must verify the identities of Alice and Bob
- The certificates must be placed in a Certificate Repository (CR)
- When they expire, they must be placed on a Certificate Revocation List (CRL)

All these things are done by Public key infrastructure (PKI)

- Creation
- Suspension
 - Certificate cannot be used while suspended
 - When an employee goes on leave
- Revocation
 - Certificate goes on Certificate Revocation List (CRL)
 - When a private key is lost
- Expiration

- **Certificate Authority (CA)**
 - An entity that issues digital certificates for others
 - A user provides information to a CA that verifies his/her identity
 - The user generates public and private keys and sends the public key to the CA
 - The CA inserts this public key into the certificate
- **Registration Authority (RA)**
 - Handles some CA tasks such as processing certificate requests and authenticating users

- **Certificate Repository (CR)**
 - A publicly accessible directory that contains the certificates and CRLs published by a CA
 - Certificate repositories store certificates so that applications can retrieve them on behalf of users.
 - The term repository refers to a network service that allows for the distribution of certificates.
 - CRs are often available to all users through a Web browser interface.
- **A management function, typically implemented via a management console.**

- **A certificate revocation list (CRL)**
 - CRL is a list of **digital certificates** that have been revoked by the issuing certificate authority (CA) before their actual or assigned expiration date.
 - It is a type of blocklist that includes certificates that should no longer be trusted and is used by various endpoints, including web browsers, to verify if a certificate is valid and trustworthy.
 - The CRL file is signed by the CA to prevent tampering.

- **Issuing certificates:** The CA signs the certificate, thereby authenticating the identity of the requestor. In addition, the CA “stamps” the certificate with an expiration date. The CA may return the certificate to the requesting system and/or post it in a repository.
- **Revoking certificates:** A certificate may become invalid before the normal expiration of its validity period. For instance, an employee may quit or change names, or a private key may be compromised. Under such circumstances, the CA revokes the certificate by including the certificate’s serial number on the next scheduled CRL.

- **Storing and retrieving certificates and CRLs:** The most common means of storing and retrieving certificates and CRLs is via a directory service, with access via LDAP.
- **Providing trust:** Organizations can establish and maintain trust within a single security management domain through a thorough audit of the CA's policies and procedures, repeated at regular intervals.

PKI standards permit multiple PKIs to interoperate, and multiple applications to interface with a single, consolidated PKI. There are two standards:

- **X.509**

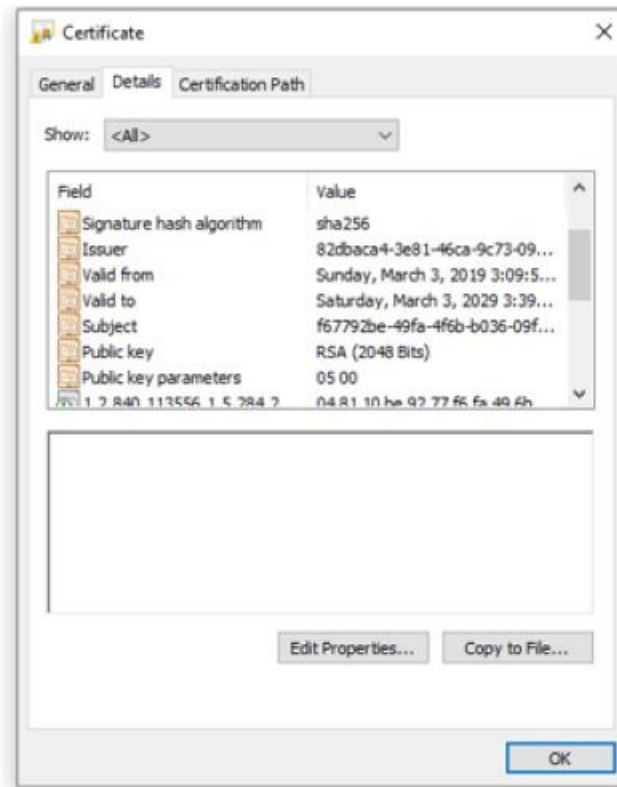
The foundational and most universally supported PKI standard is the International Telecommunication Union (ITU) ITU's X.509. The primary purpose of X.509 is to define a standard digital certificate format.

- **PKCS**

PKCS is a series of standards covering PKI in areas of certificate enrolment and renewal and CRL distribution. For PKI interoperability, the three most important PKCS standards are PKCS #7, "Cryptographic Message Syntax Standard," PKCS #10, "Certificate Request Syntax Standard," and PKCS #12, "Personal Information Exchange Syntax Standard".

Field Name	Explanation
Certificate version number	0=Version 1, 1=Version 2, 2=Version 3
Serial number	Unique serial number of certificate
Issuer signature algorithm ID	"Issuer" is Certificate Authority
Issuer X.500 name	Certificate Authority name
Validity period	Start date/time and expiration date/time
Subject X.500 name	Private key owner
Subject public key information	Algorithm ID and public key value
Issuer unique ID	Optional; added with Version 2
Subject unique ID	Optional; added with Version 2
Extensions	Optional; added with Version 3
Signature	Issuer's digital signature

Selected X.509 Digital Certificate Fields



- A numbered set of PKI standards that have been defined by the RSA Corporation
- These standards are based on the RSA public-key algorithm

PKCS Standard Number	Current Version	PKCS Standard Name	Description
PKCS #1	2.1	RSA Cryptography Standard	Defines the encryption and digital signature format using RSA public key algorithm
PKCS #2	N/A		Originally defined the RSA encryption of the message digest; now incorporated into PKCS #1
PKCS #3	1.4	Diffie-Hellman Key Agreement Standard	Defines the secret key exchange protocol using the Diffie-Hellman algorithm
PKCS #4	N/A		Originally defined specifications for the RSA key syntax; now Incorporated into PKCS #1
PKCS #5	2.0	Password-Based Cryptography Standard	Describes a method for generating a secret key based on a password; known as the password-based encryption standard (PBE)
PKCS #6	1.5	Extended-Certificate Syntax Standard	Describes an extended-certificate syntax; currently being phased out
PKCS #7	1.5	Cryptographic Message Syntax Standard	Defines a generic syntax for defining digital signature and encryption
PKCS #8	1.2	Private-Key Information Syntax Standard	Defines the syntax and attributes of private keys; also defines a method for storing keys
PKCS #9	2.0	Selected Attribute Types	Defines the attribute types used in data formats defined in PKCS #6, PKCS #7, PKCS# 8, and PKCS #10
PKCS #10	1.7	Certification Request Syntax Standard	Outlines the syntax of a request format sent to a CA for a digital certificate

- **Certificate policy (CP)**
 - A published set of rules that govern the operation of a PKI
 - Provides recommended baseline security requirements for the use and operation of CA, RA, and other PKI components
- **Certificate practice statement (CPS)**
 - Describes in detail how the CA uses and manages certificates
 - A more technical document than a CP

Trust may be defined as confidence in or reliance on another person or entity

- **Trust model**

- Refers to the type of trusting relationship that can exist between individuals or entities

- **Direct trust**

- A relationship exists between two individuals because one person knows the other person

- **Third-party trust**

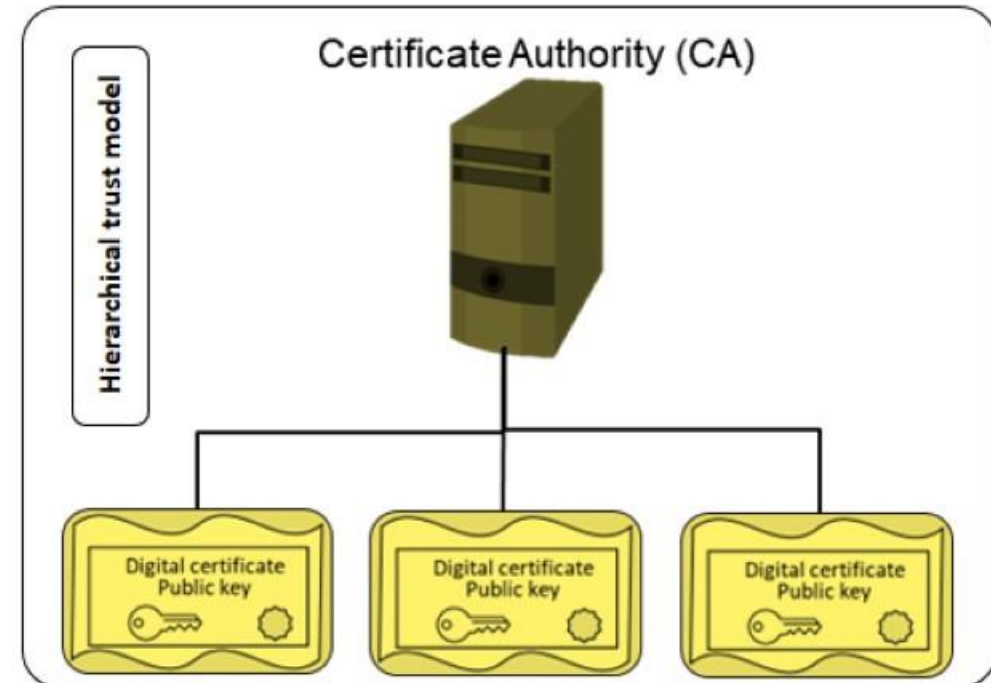
- Refers to a situation in which two individuals trust each other because each trusts a third party

Two PKI trust models that use a CA

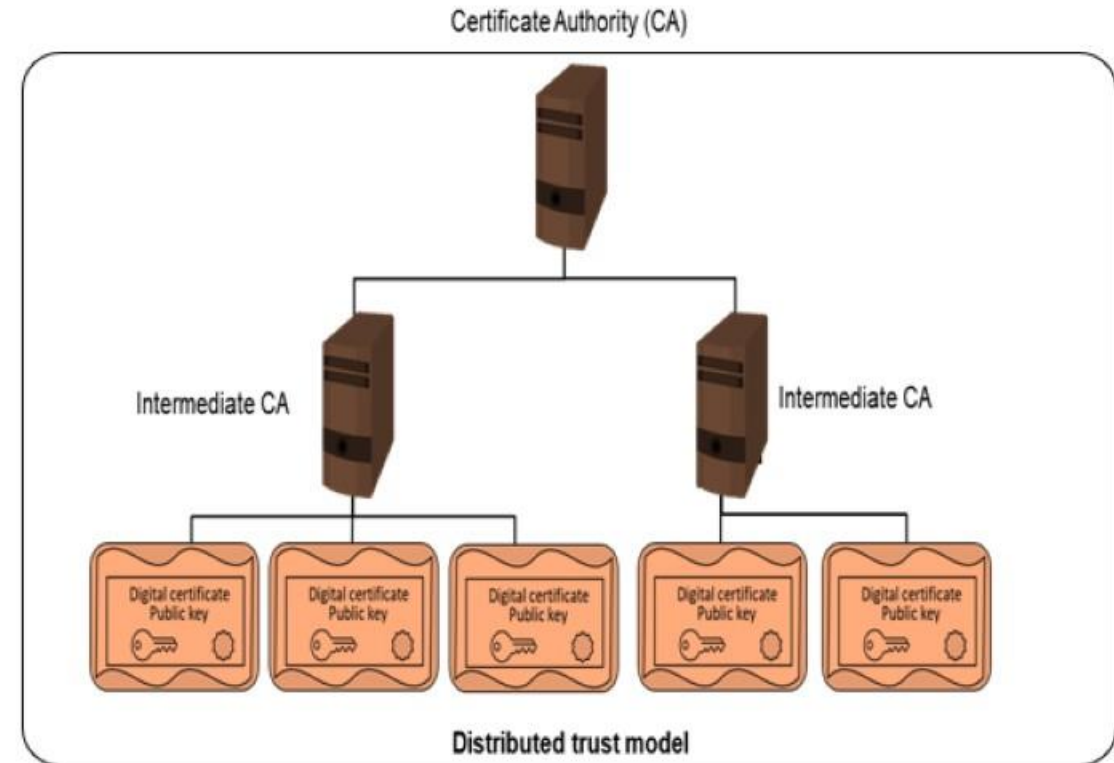
Hierarchical trust model

Distributed trust model

- One master "root" CA signs all digital certificates with a single private key
- Limitation: If root CA's private is compromised, all digital certificates signed would be worthless



- The distributed trust model contains numerous series of CAs that can sign the digital certificates rather than a single CA as in a hierarchical trust model. As a result, the drawbacks of a hierarchical trust model are essentially eliminated.
- The responsibility for verifying the digital certificates can be distributed, and the loss of the CA's private key would only risk those digital certificates for which it had been signed by the compromised CA.
- In addition, the CA can delegate authority to another intermediate CA to sign digital certificates.



- **File Transfer Protocol (FTP)**
 - Part of the TCP/IP suite
 - Used to connect to an FTP server
- Vulnerabilities
 - Usernames, passwords, and files being transferred are in cleartext
 - Files being transferred by FTP are vulnerable to man-in-the-middle attacks
- One of the ways to reduce the risk of attack is to use encrypted **Secure FTP (SFTP)**

- **Secure Sockets Layer (SSL)**
 - A protocol developed by Netscape for securely transmitting documents over the Internet
 - Uses a public key to encrypt data that is transferred over the SSL connection
- **Transport Layer Security (TLS)**
 - A protocol that guarantees privacy and data integrity between applications communicating over the Internet
 - An extension of SSL
- Are often referred to as SSL/TLS or TLS/SSL)

Protocols that Rely on a PKI (Cont.)

Secure Shell (SSH)

- A second protocol that can be used with SFTP is **Secure Shell (SSH)**
 - Also called SFTP/SSH
- SSH
 - A UNIX-based command interface and protocol for securely accessing a remote computer
 - Suite of three utilities: slogin, scp, and ssh
 - Both the client and server ends of the connection are authenticated using a digital certificate
 - Passwords are protected by being encrypted

- **S/MIME (Secure/Multipurpose Internet Mail Extensions)**
 - One of the most common e-mail transport protocols
 - Uses digital certificates to protect the e-mail messages
- S/MIME functionality is built into most of the modern e-mail software and interoperates between them

Challenges that a PKI Solves:

PKI's popularity is owed to the different issues that it resolves. Several PKI use cases include:

- SSL/TLS certifications are used to secure communication networks and web browsers.
- Encryption of Data
- Software with a digital signature
- Access to WiFi without passwords

- Speed:** To generate a safe key pair, PKI employs extremely sophisticated algorithms. Consequently, the procedure and data transfer gradually get slower.
- Private Key Compromise:** Although PKI is difficult to hack, a private key can be. Since PKI combines a user's private key and a public key to encrypt and decrypt data, the information can be quickly decrypted with the user's private key in hand and the public key, which is easily accessible.

Understanding Public Key Infrastructure (PKI) An RSA Data Security White Paper. https://paper.bobyline.com/System/understanding_pki.pdf

Stallings, W. (2006). Cryptography and network security principles and practices 4th edition



Thank You