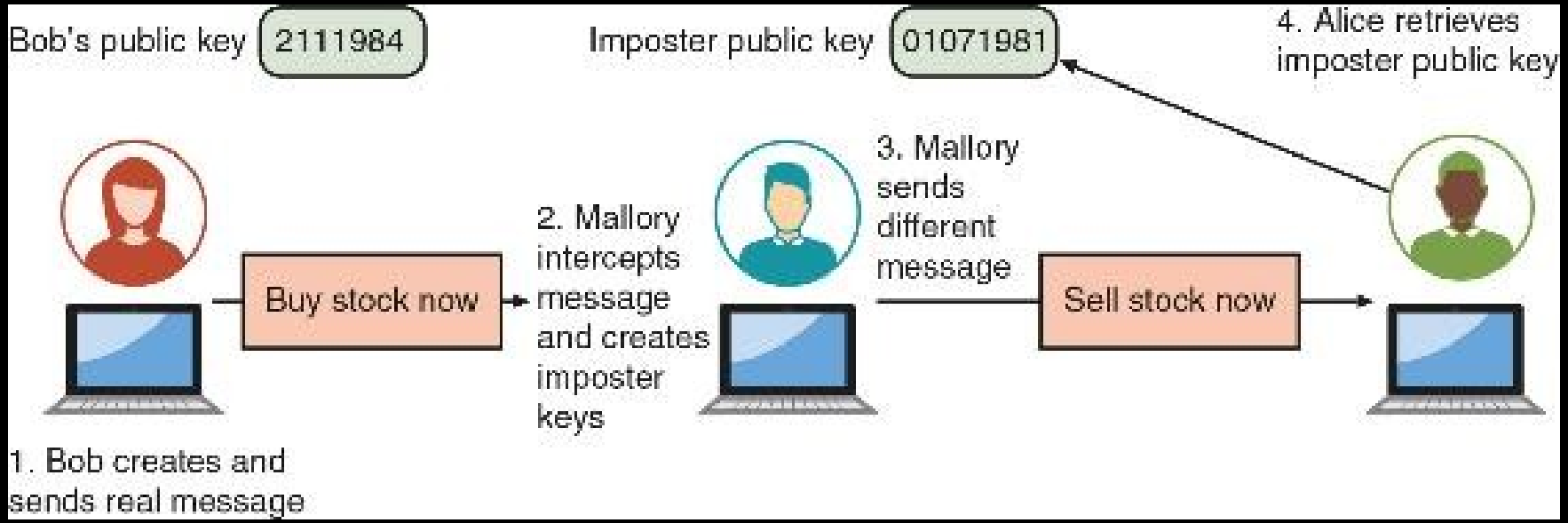
Chapter 4: Advanced Cryptography

Defining Digital Certificates

- A digital signature is used to prove a document originated from a valid sender
- There is a weakness with a digital signature: it can only prove that the private key of the sender was used to encrypt the digital signature
  - An imposter could post a public key under a sender's name
- A trusted **third party** can be used to help solve the problem of verifying identity
- A **digital certificate** is a technology used to associate a user's identity to a public key that has been "digitally signed" by a trusted third party

Imposter Public Key



Managing Digital Certificates

- Entities and technologies used to manage digital certificates include:
  - **Certificate authorities (CAs)** and tools for managing certificates
- If a user wants a digital certificate, after generating a public and private key, the user must complete a request
  - The user electronically signs it by affixing their public key and sends it to a **registration authority** that is responsible for verifying the authenticity of the user
  - Once verified, it is transferred to an intermediate certificate authority where the request is processed and a digital certificate is issued (a process known as **certificate signing request (CSR) generation**)

Managing Digital Certificates

- Intermediate CAs are subordinate entities designed to handle specific CA tasks such as processing certificate requests and verifying the identity of the individual
- The person requesting a digital certificate can be authenticated by the following methods:
  - Email, documents, in person
- A **certificate repository (CR)** is a publicly accessible centralized directory of digital certificates used to view certificate status
  - This directory can be managed locally by setting it up as a storage area connected to the CA server

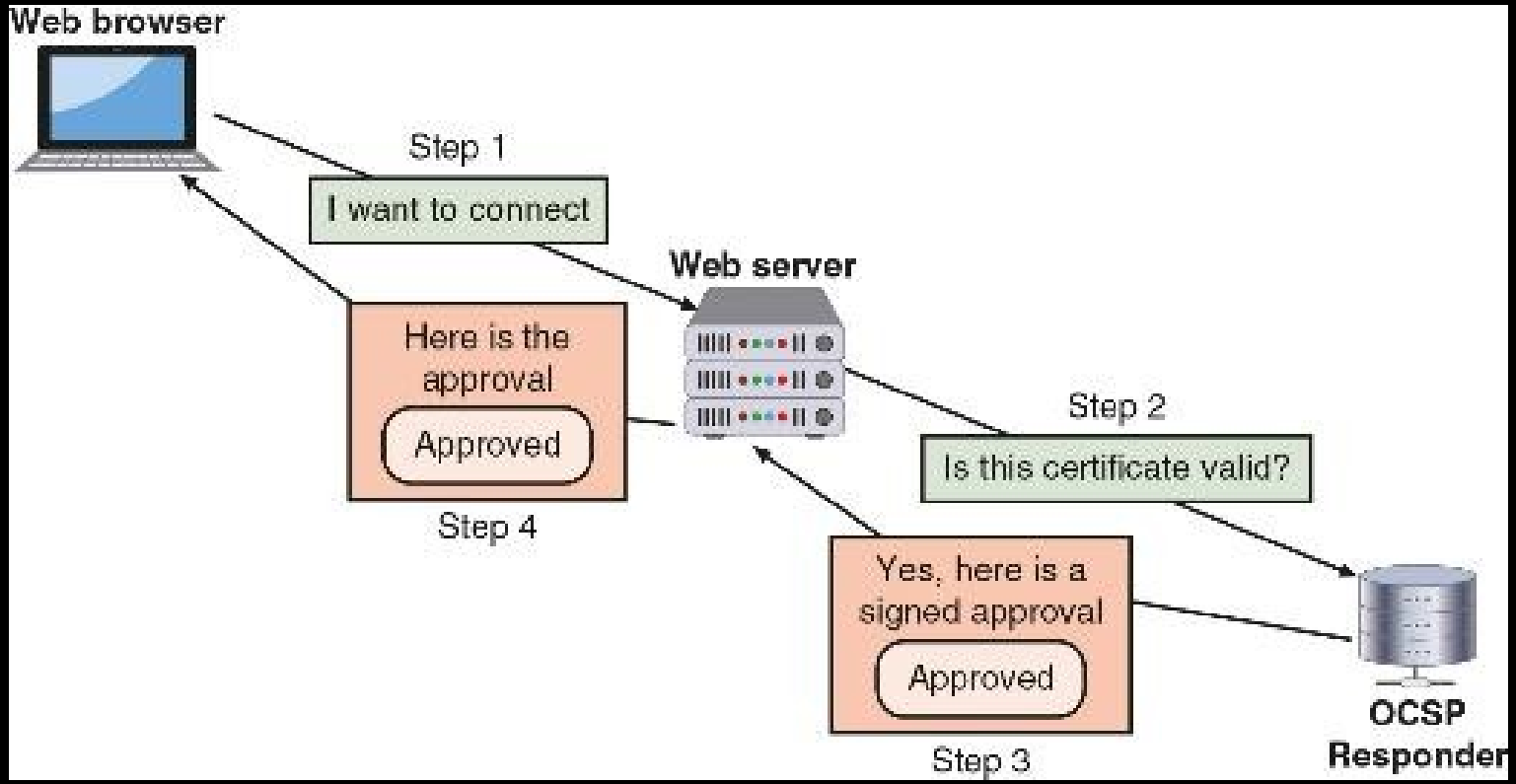
Managing Digital Certificates

- Some circumstances might cause a certificate to be revoked, such as the following:
  - Certificate is no longer used
  - Details of the certificate have changed, such as the user's address
  - Private key has been lost or exposed (or suspected lost or exposed)
- A **Certificate Revocation List** (**CRL**) is a list of digital certificates that have been revoked

Managing Digital Certificates

- The **Online Certificate Status Protocol** (**OCSP**) performs a real-time lookup of a certificate's status
  - The browser sends the certificate's information to a trusted entity known as an OCSP Responder
  - The OCSP Responder provides immediate revocation information on that certificate
- **OCSP stapling** is a variation of OCSP where web servers send queries to the OCSP Responder server at regular intervals to receive a signed time-stamped response

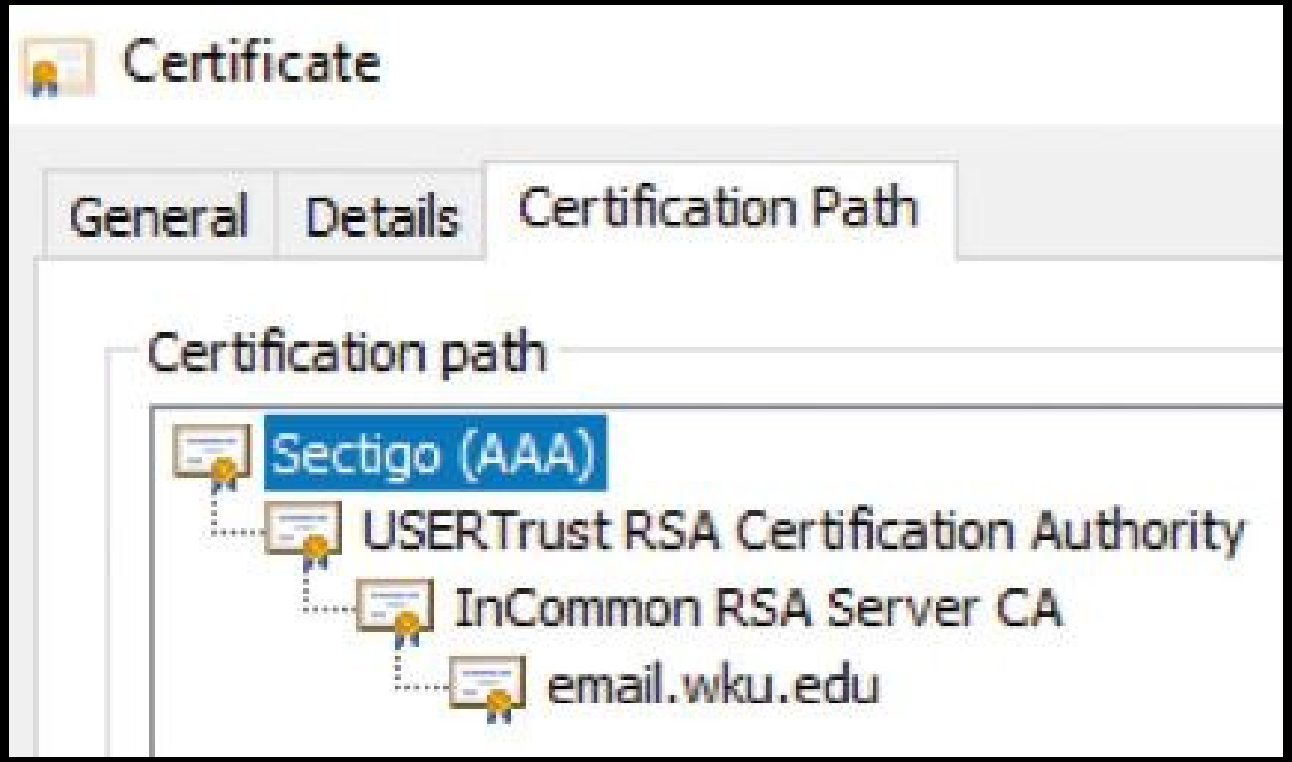
OSCP Stapling



Types of Digital Certificates

- The most common categories of digital certificates are root certificates, domain certificates, and hardware/software certificates
- The process of verifying a digital certificate is genuine depends upon **certificate chaining**
  - The beginning point of the chain is known as a **root digital certificate** and is created and verified by a CA
  - They are **self-signed** and do not depend upon any higher-level authority
  - The endpoint of the chain is the **user digital certificate** itself

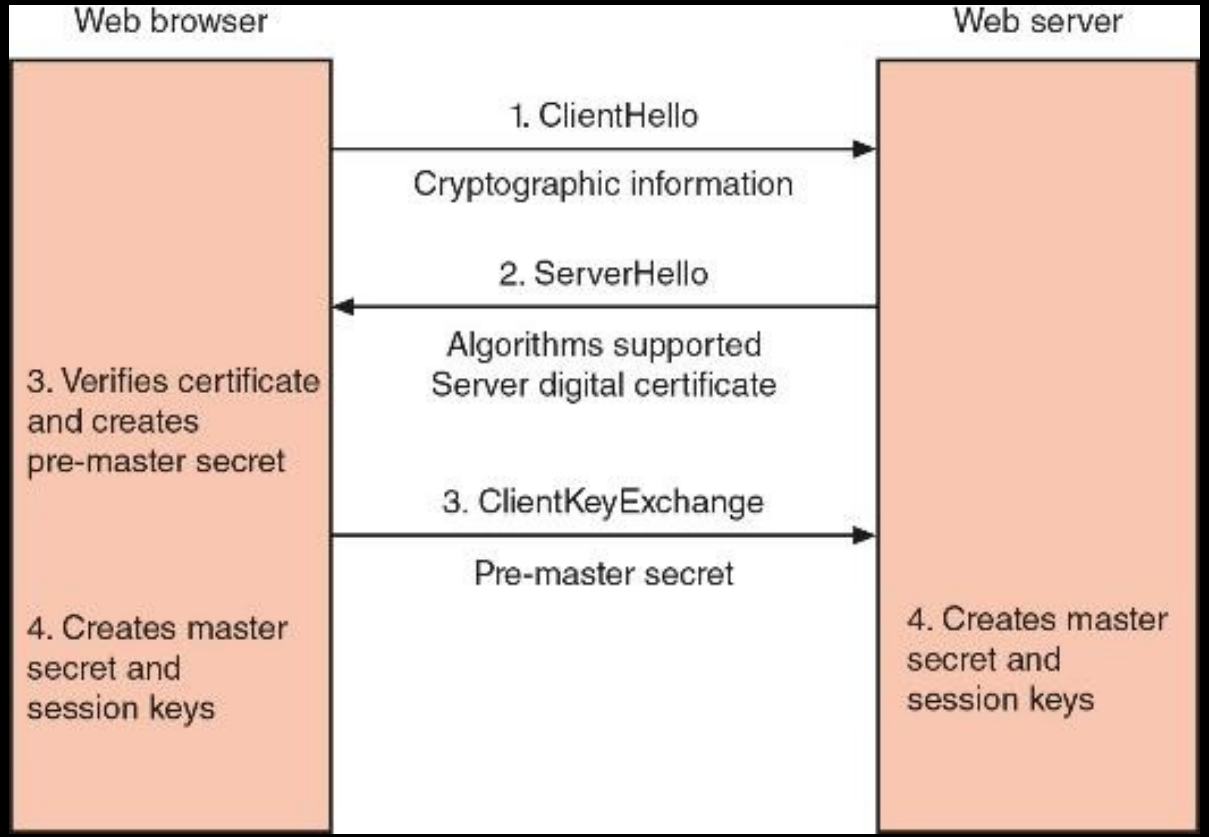
Example of Certificate Chaining



Types of Digital Certificates

- Most digital certificates are web server digital certificates
- Web server digital certificates perform two primary functions:
  - Ensure the authenticity of the web server to the client
  - Ensure the authenticity of the cryptographic connection to the web server
- There are several types of domain digital certificates: domain validation digital certificates, extended validation (EV) digital certificates, wildcard digital certificates, and subject alternative name (SAN) digital certificates

Key Exchange



Types of Digital Certificates

- Hardware and Software Digital Certificates
- More specific digital certificates relate to hardware and software:
  - **Machine/computer digital certificate**
  - **Code signing digital certificate**
  - **Email digital certificate**

Types of Digital Certificates

- Digital Certificate Attributes and Formats
  - The standard format for digital certificates is X.509 Version 3
  - Several certificate attributes make up an X.509 digital certificate including the following:
    - The certificate validity period
    - End-host identity information
    - Encryption keys that will be used for secure communications
    - The signature of the issuing CA
    - The common name (CN) of the device being protected

Question?

- What is a technology used to associate a user’s identity to a public key and has been digitally signed by a trusted third party?

Answer

- What is a technology used to associate a user’s identity to a public key and has been digitally signed by a trusted third party?
- A digital certificate is a technology used to associate a user’s identity to a public key and has been digitally signed by a trusted third party.

What is Public Key Infrastructure?

- There is a need for a consistent means to manage digital certificates
- **Public key infrastructure (PKI)** is a framework for all entities involved in digital certificates
- It is the set of software, hardware, processes, procedures, and policies that are needed to create, manage, distribute, use, store, and revoke digital certificates across large user populations

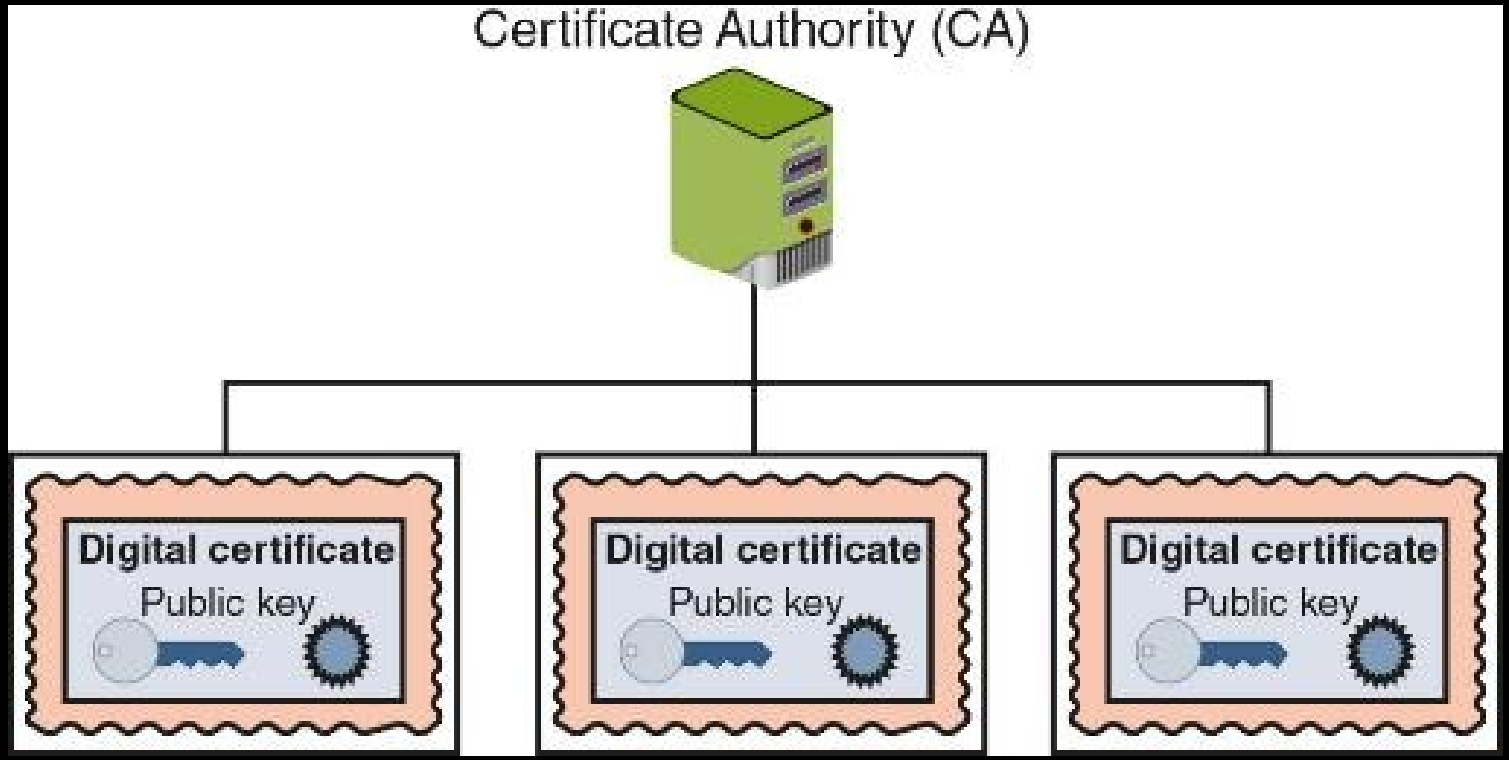
Trust Models

- **Trust** is defined as confidence in or reliance on another person/entity
- A **trust model** refers to the type of trust relationship that can exist between individuals and entities
- **Direct trust** is a type of trust model where one person knows the other person
- **Third-party trust** refers to a situation where two individuals trust each other because each trusts a third party
- The **web of trust** model is based on direct trust, where each user signs a digital certificate then exchanges certificates with all other users

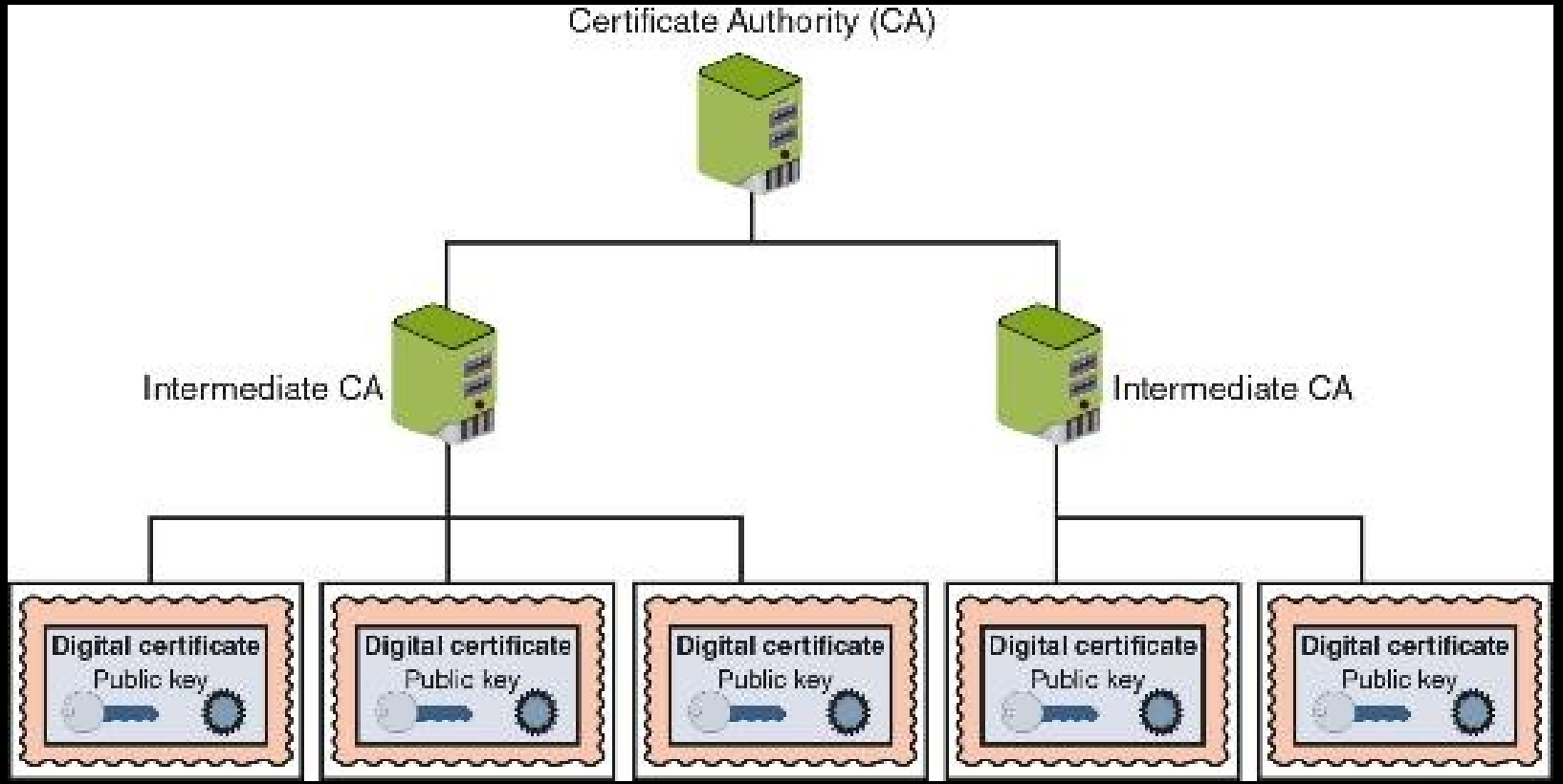
Trust Models

- The **hierarchical trust model** assigns a single hierarchy with one master CA called the **root**
  - The root signs all digital certificate authorities with a single key
- The **distributed trust model** has multiple CAs that sign digital certificates
  - It eliminates limitations of hierarchical trust model
- The **bridge trust model** is similar to the distributed trust model
  - One CA acts as a facilitator to interconnect all other CAs
  - Allows different models to be linked together

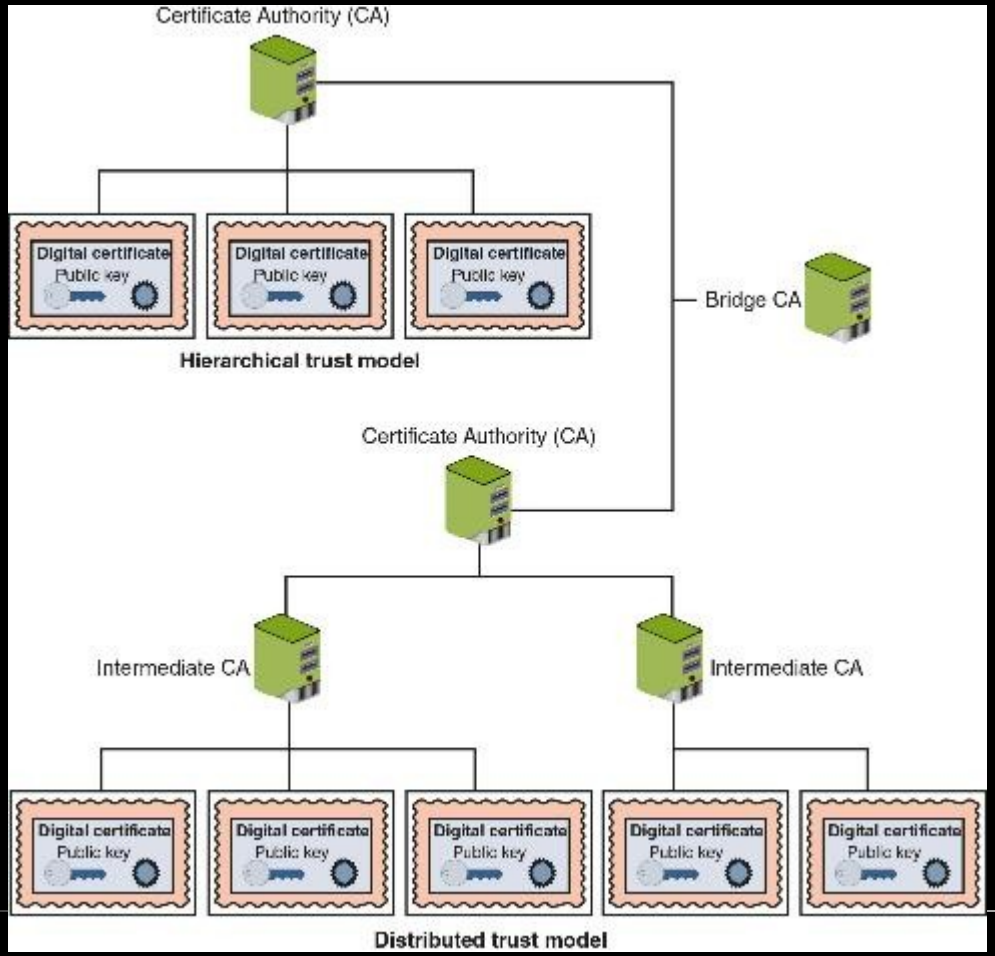
Hierarchical Trust Model



Distributed Trust Model



Bridge Trust Model



Managing PKI

- A **certificate policy** (**CP**) is a published set of rules that govern operation of a PKI
  - The CP provides recommended baseline security requirements for the use and operation of CA, RA, and other PKI components
- A **certificate practice statement** is a technical document that describes in detail how the CA uses and manages certificates
  - It also covers how to register for a digital certificate, how to issue them, when to revoke them, procedural controls and key pair management

Managing PKI

- The life cycle of a certificate is typically divided into the following four parts:
  - Creation
  - Suspension
  - Revocation
  - Expiration

Key Management

- Public keys can be stored by embedding them within digital certificates
- Private keys can be stored on the user's local system
  - Software-based storage may expose keys to attackers
  - An alternative is to store keys in hardware on smart-cards or tokens
- Multiple pairs of dual keys can be created
  - One pair is used to encrypt information and the public key can be backed up to another location
  - The second pair would be used only for digital signatures and the public key in that pair would never be backed up

Key Management

- The following procedures can help ensure keys are handled properly:
  - Escrow
  - Expiration
  - Renewal
  - Revocation
  - Recovery
  - Suspension
  - Destruction

Question?

- Dag wants to set up a trust model in which he only will serve as a CA. Which trust model will he choose?

Answer

- Dag wants to set up a trust model in which he only will serve as a CA. Which trust model will he choose?
- A hierarchical trust model can be used in an organization where one CA is responsible for only the digital certificates for that organization.

Secure Communication

- Cryptographic algorithms are used to protect data in transit (transport/communication encryption)
- There are different secure communication and transport protocols based on cryptographic algorithms for protecting data in transit
  - These protocols typically rely on “encapsulating” or enveloping the data to be transmitted inside something else (tunneling)
- The following protocols use tunneling:
  - Transport Layer Security (TLS) and IP Security (IPSec)

Transport Layer Security (TLS)

- **Transport Layer Security (TLS)** is a replacement for Secure Sockets Layer (SSL) and provides a higher degree of protection
  - The current version is TLS v1.3
- A **cipher suite** is a named combination of the encryption, authentication, and message authentication code (MAC) algorithms that is used with TLS

IP Security (IPSec)

- **IPSec** is a protocol suite for securing IP communications
- IPSec is considered to be a transparent security protocol
  - Transparent to applications, users, and software
- IPSec provides three areas of protection that correspond to three IPSec protocols:
  - *Authentication, confidentiality, and key management*
- IPSec supports two encryption modes:
  - Transport mode and tunnel mode

Other Protocols

- The secure version of HTTP is actually "*plain*" HTTP sent over TLS and is called **Hypertext Transport Protocol Secure** (**HTTPS**)
  - HTTPS uses port 443 instead of HTTP's port 80
- **Secure Shell** (**SSH**) is an encrypted alternative to the Telnet protocol used to access remote computers
- **Secure/Multipurpose Internet Mail Extensions** (**S/MIME**) is a protocol for securing email messages
- **Secure Real-time Transport Protocol** (**SRTP**) is a secure extension protecting transmission using the Real-Time Transport Protocol (RPT)

Implementing Cryptography

- Cryptography that is improperly applied can lead to vulnerabilities
- It is essential to understand the different options that relate to cryptography
- Implementing cryptography includes understanding the following:
  - Key strength
  - Secret algorithms
  - Block cipher modes of operation

Key Strength

- A cryptographic key is a value that serves as input to an algorithm
  - It transforms plaintext into ciphertext (and vice versa for decryption)
- The following are primary characteristics that determine the resiliency of the key to attacks (called **key strength**):
  - Randomness
  - Cryptoperiod – length of time for which a key is authorized for use
  - Length of the key

Secret Algorithms

- Keys must be kept secret, so does the same apply to algorithms?
- Would a secret algorithm enhance security in the same way as keeping a key or password secret?
  - No
- For a cryptography to be useful it needs to be widespread:
  - A military force that uses cryptography must allow many users to know of its existence to use it

Block Cipher Modes of Operation

- A block cipher manipulates an entire block of plaintext at one time
  - Each block is encrypted independently
- A **block cipher mode of operation** specifies how block ciphers should handle these blocks
- Some of the most common modes:
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
  - Counter (CTR)
  - Galois/Counter (GCM)