ĐẠI HỌC
BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY
OF SCIENCE AND TECHNOLOGY

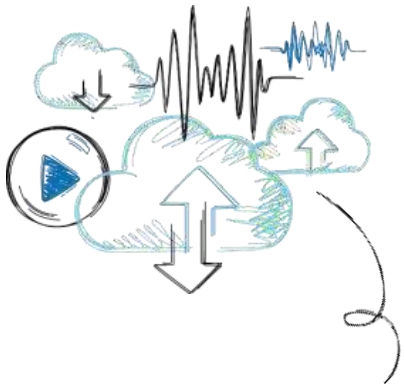
CS4451 – Computer Security

Advanced Cryptography and PKI

Dr. Luu Quang Trung
trung.luuquang@hust.edu.vn

ONE LOVE. ONE FUTURE.

Objectives



1. Explain how to implement cryptography
2. Define digital certificates
3. Describe the components of Public Key Infrastructure (PKI)
4. Describe the different transport encryption protocols

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:
    - Key strength
    - Secret algorithms
    - Block cipher modes of operation
    - Cryptographic service providers
    - The use of algorithm input values

Key Strength (1 of 2)

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

Key Strength (2 of 2)

Key length	Key space	Average number of attempts needed to break
3	17,576	8788
4	456,976	228,488
5	11,881,376	5,940,688
6	308,915,776	154,457,888
7	8,031,810,176	4,015,905,088
8	208,827,064,576	104,413,532,288

Secret Algorithms

- Would a secret algorithm enhance security in the same way as keeping a key or password secret? No.
  - keeping a secret algorithm can add a layer of obscurity, but it's not a substitute for a strong, well-tested encryption algorithm. The real security comes from keeping the key secret, and relying on a well-established algorithm that has been vetted by the security community.
- 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

Algorithm: Design of the lock

Block Cipher Modes of Operation

- A block cipher manipulates an entire block of plaintext at one time
  - The plaintext is divided into separate blocks of specific lengths
  - Each block is encrypted independently
- Block cipher mode of operation
  - Specifies how block ciphers should handle these blocks
- Most common modes:
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
  - Counter (CTR)
  - Galois/Counter (GCM)

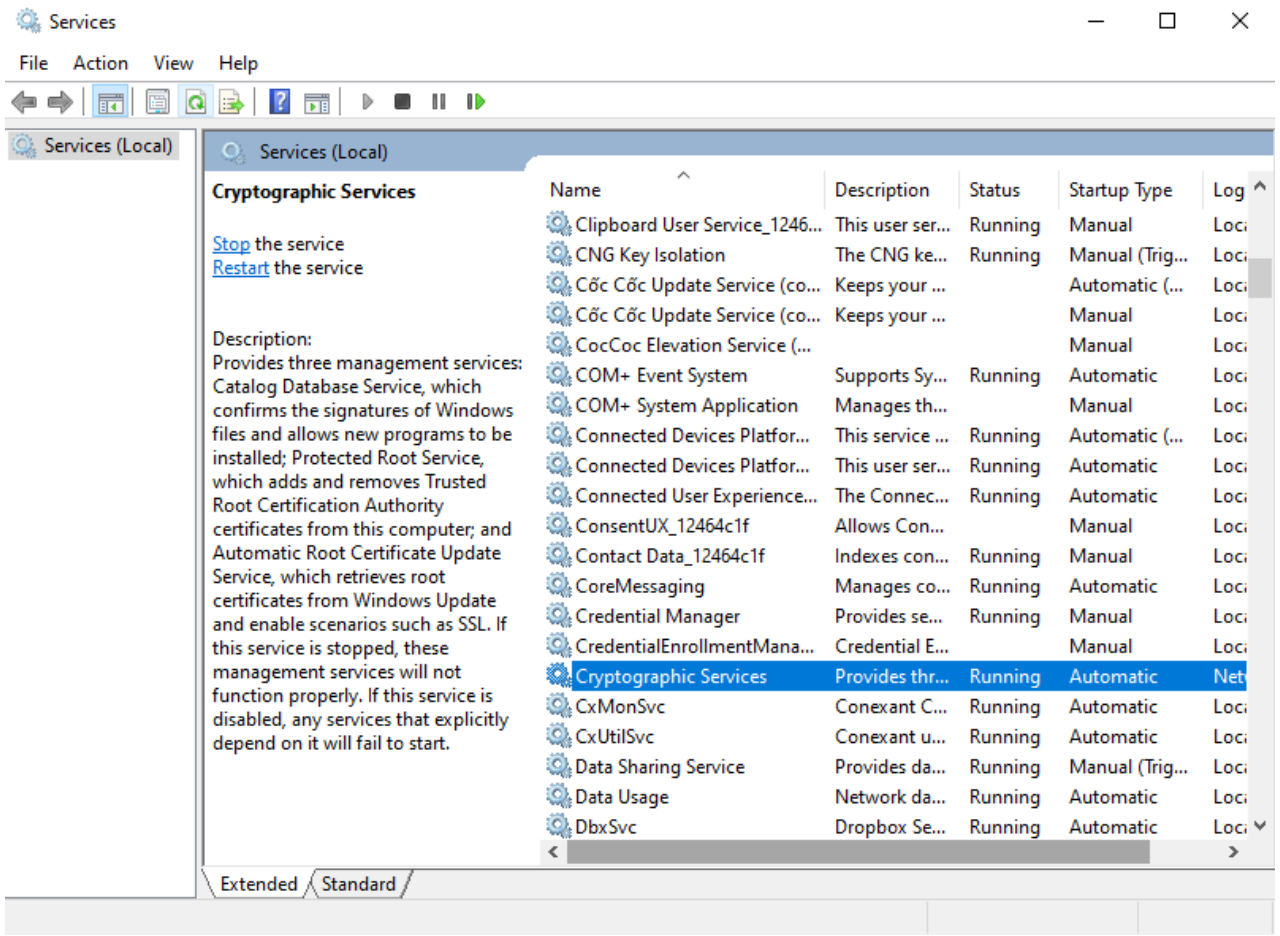
Crypto Service Providers (1 of 2)

- Crypto service provider
    - Allows an application to implement an encryption algorithm for execution
- Crypto service providers typically:
    - Implement cryptographic algorithms
    - Generate keys
    - Provide key storage
    - Authenticate users by calling various crypto modules to perform specific tasks
- Crypto service providers can be implemented in:
    - Software, hardware, or both

Crypto Service Providers (2 of 2)

Microsoft Cryptographic Services in Windows 10:

Start > Services > Enter



Algorithm Input Values

- Some cryptographic algorithms require that in addition to a key another value can or must be input
  - May be called algorithm input values
- **Salt**
  - A value that can be used to ensure that plaintext, when hashed, will not consistently result in the same digest
  - Most often used in password-based systems
- **Nonce**
  - An input value that must be unique within some specified scope
- **Initialization vector (IV)**
  - Most widely used algorithm input

Digital Certificates

- Digital Certificates
    - A common application of cryptography
- Using digital certificates involves
    - Understanding their purpose
    - Knowing how they are managed
    - Determining which type of digital certificate is appropriate for different situations

Defining Digital Certificates (1 of 3)

- Digital signature
    - Used to prove a document originated from a valid sender
- Weakness of using digital signatures
    - They only show that the private key of the sender was used to encrypt the digital signature
    - Imposter could post a public key under a sender's name

Imposter /im'pɔstə/: kẻ lừa đảo, kẻ mạo danh

Defining Digital Certificates (2 of 3)

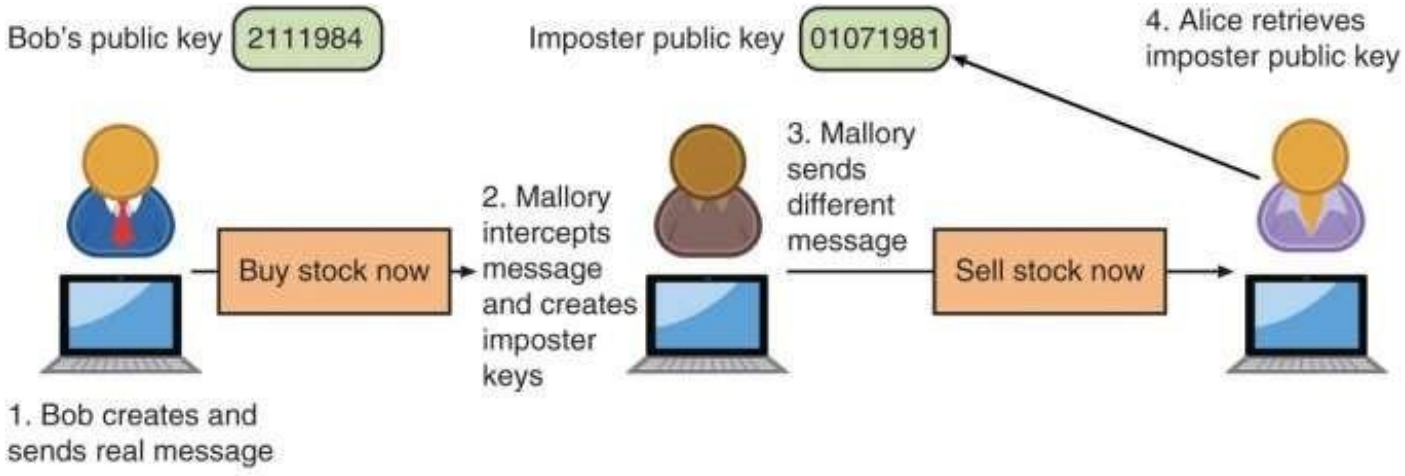


Figure 4-2 Imposter public key

- **Mallory** creates a new RSA key pair, keeps the private key, and forges the public key to appear as **Bob**'s
- **Mallory** sends the fake public key to **Alice** by spoofing **Bob**'s website or email.

- **Alice**, believing the public key to be **Bob**'s, uses it to encrypt her email
- **Mallory** leverages her private key to decrypt **Alice** 's email and access its content

Defining Digital Certificates (3 of 3)

- **Trusted third party**
  - Used to help solve the problem of verifying identity
  - Verifies the owner and that the public key belongs to that owner
  - Helps prevent man-in-the-middle attack that impersonates owner of public key
- 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

Managing Digital Certificates

- Several entities and technologies are used to manage digital certificates:
    - Certificate authorities (CAs)
    - Tools for managing certificates

Certificate Authorities (1 of 3)

- Certificate authority (CA)
  - Responsible for digital certificates
  - May also be called **root CA**
- If a user wants a digital certificate:
  - After generating a public and private key, user must complete a request with information such as name, address, email address, etc.
  - Known as a Certificate Signing Request (CSR)
- User electronically signs the CSR and sends it to an intermediate CA
  - Intermediate CA processes the CSR and verifies the authenticity of the user

Certificate Authorities (2 of 3)

Car title scenario	Digital certificate element	Explanation
Car title application	Certificate Signing Request (CSR)	Formal request for digital certificate
Sign car title application	Create and affix public key to certificate	Added to digital certificate for security
Visit county courthouse	Intermediate certificate authority	Party that can process CSR on behalf of CA
Title sent from state DMV	Certificate authority (CA)	Party responsible for digital certificates

Certificate Authorities (3 of 3)

- Intermediate CAs are subordinate entities designed to handle specific C A tasks such as:
  - Processing certificate requests
  - Verifying the identity of the individual
- The person requesting a digital certificate can be authenticated by:
  - Email, documents, in person
- A common method to ensure security and integrity of a root CA:
  - Keep it in an offline state from the network (offline CA)
- It is only brought online (online CA) when needed for specific and infrequent tasks

Certificate Management (1 of 4)

- **Certificate Repository (CR)**
  - Publicly accessible centralized directory of digital certificates
  - Can be used to view certificate status
  - Can be managed locally by setting it up as a storage area connected to the CA server
- **Certificate Revocation**
  - Lists of digital certificate that have been revoked
  - Reasons a certificate would be revoked
    - Certificate is no longer used
    - Details of the certificate have changed, such as user's address
    - Private key has been lost or exposed (or suspected lost or exposed)
  - **Certificate Revocation List (CRL)**
    - A list of certificate serial numbers that have been revoked

Certificate Management (2 of 4)

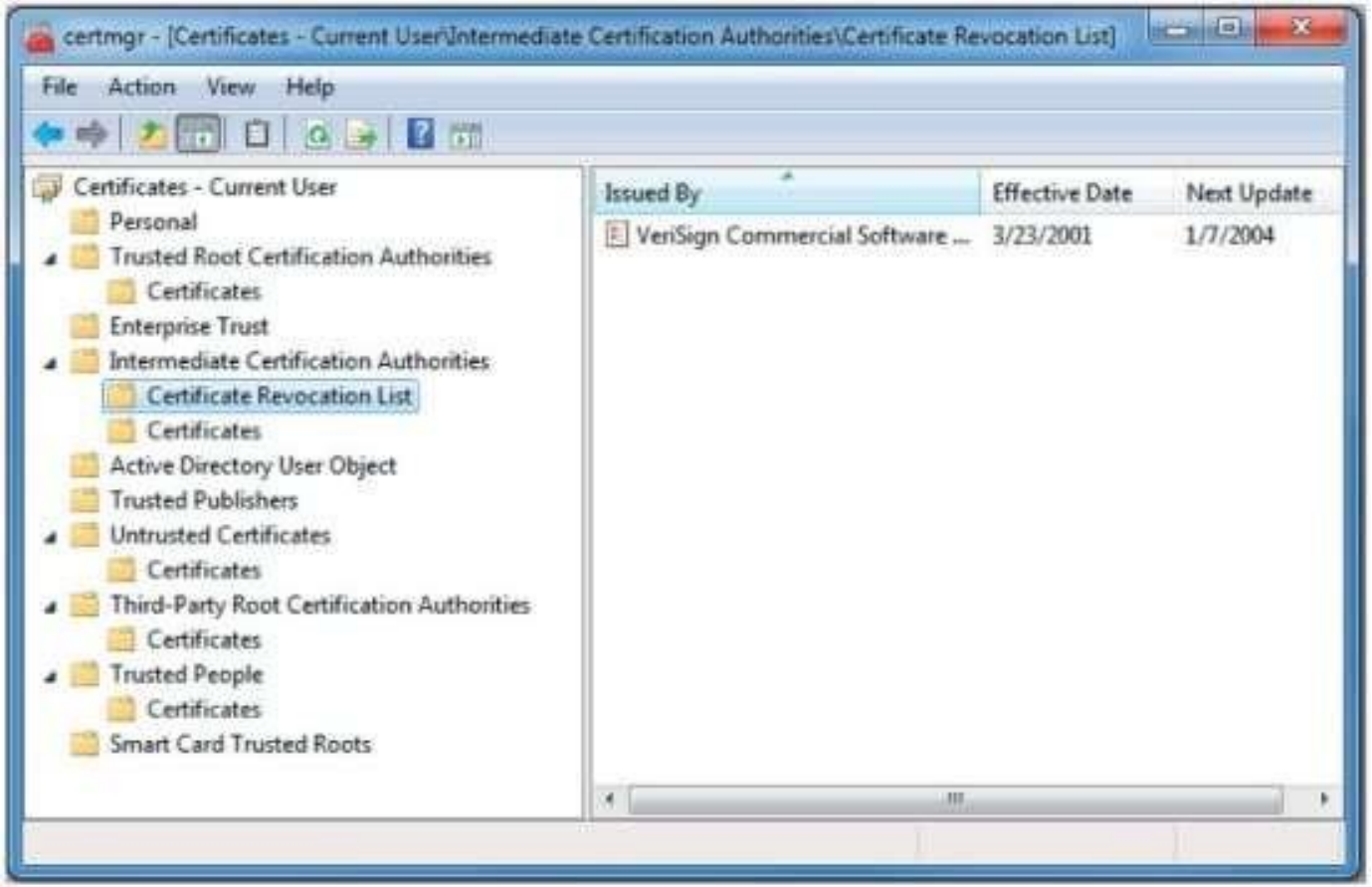


Figure 4-3 Certificate Revocation List (CRL)

Certificate Management (3 of 4)

- **Online Certificate Status Protocol (OCSP)**
  - Performs a real-time lookup of a certificate's status
  - Called a request-response protocol
  - 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**
  - A variation of OCSP where web servers send queries to the OCSP Responder server at regular intervals to receive a signed time- stamped response

Certificate Management (4 of 4)

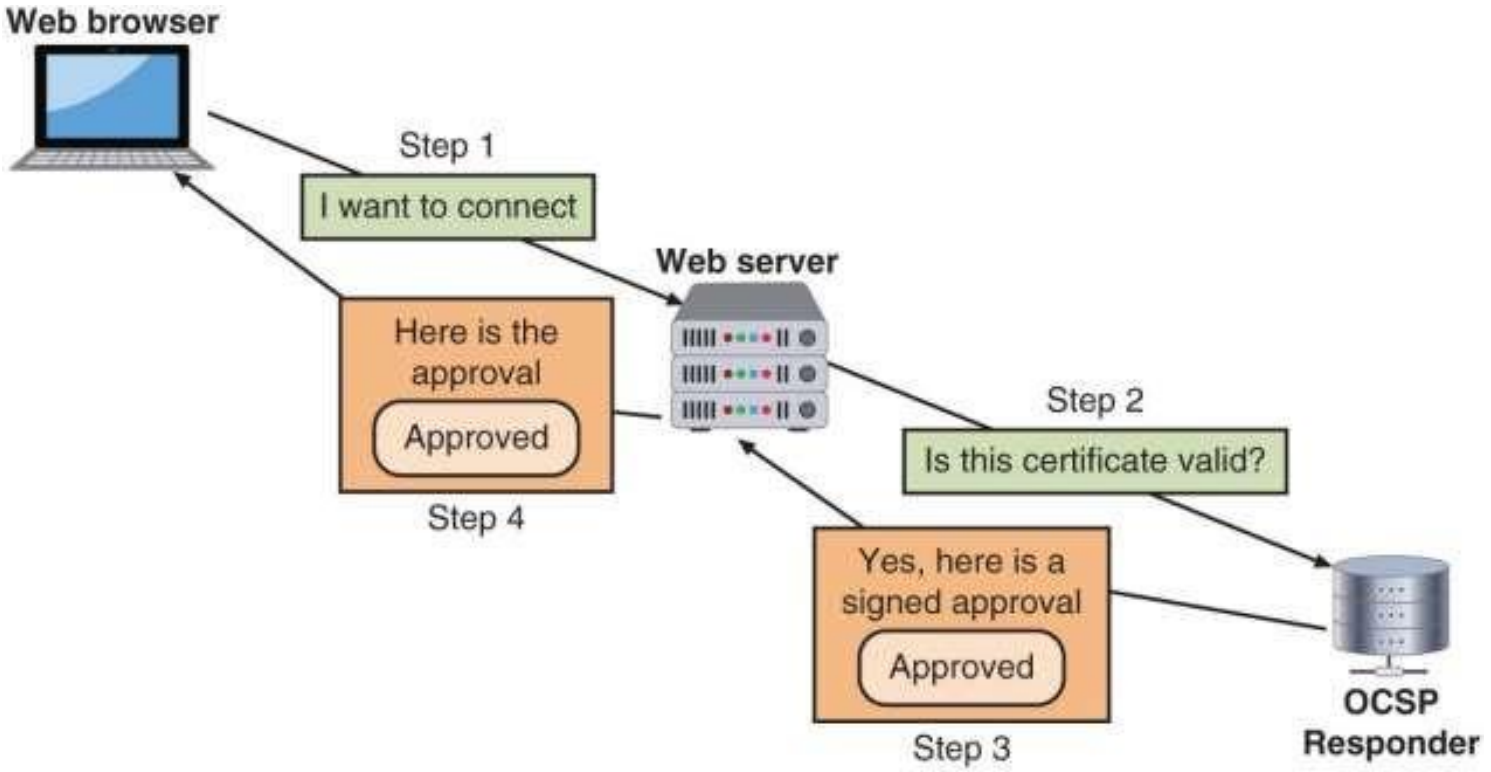


Figure 4-4 OCSP stapling

Types of Digital Certificates

- Different categories of digital certificates
- The most common categories are:
    - Root certificates
    - Domain certificates
    - Hardware and software certificates

Root Digital Certificates (1 of 4)

- The process of verifying a digital certificate is genuine depends upon **certificate chaining**
  - Links several certificates together to establish trust between all the certificates involved
  - Endpoint of the chain is the **user digital certificate** itself
- The beginning point of the chain is known as a **root digital certificate**
  - Created and verified by a CA
  - Self-signed and do not depend upon any higher-level authority
- Between root digital certificate and the user certificate can be
  - One or more intermediate certificates issued by intermediate CAs

Root Digital Certificates (2 of 4)

Figure 4-5 Certificate chaining

Root Digital Certificates (3 of 4)

Figure 4-7 Certificate chaining for cengage.com

Root Digital Certificates (4 of 4)

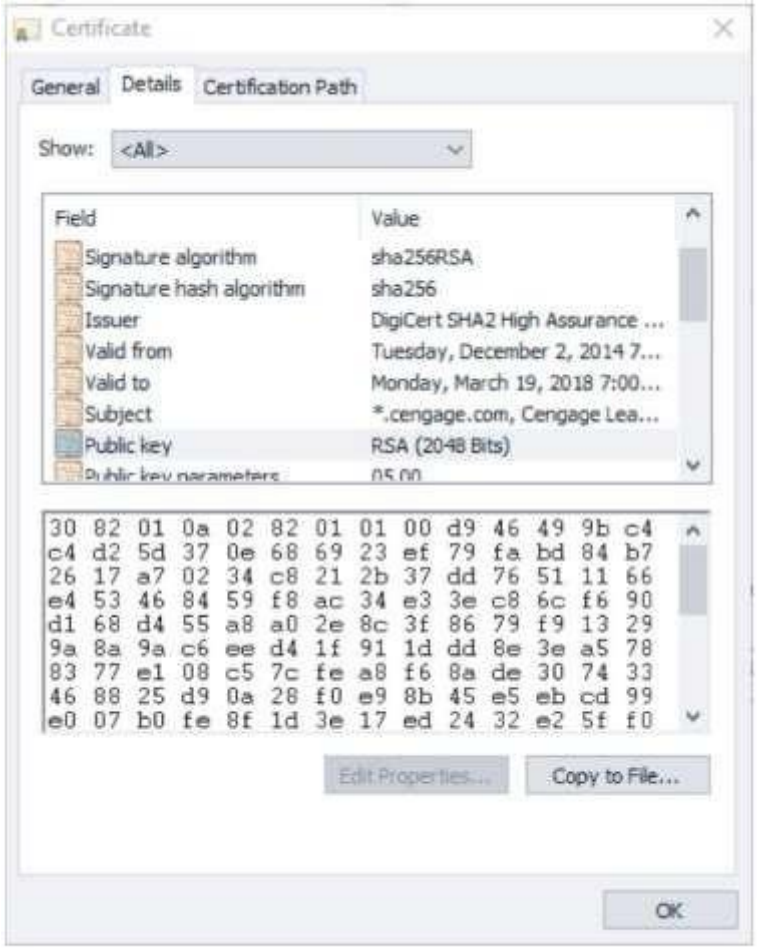


Figure 4-8 Certificate details

Domain Digital Certificates (1 of 5)

- Most digital certificates are web server digital certificates issued from a web server to a client
- 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
- Several types of domain digital certificates:
    - Domain validation digital certificates
    - Extended validation digital certificates
    - Wildcard digital certificates
    - Subject alternative names digital certificates

Domain Digital Certificates (2 of 5)

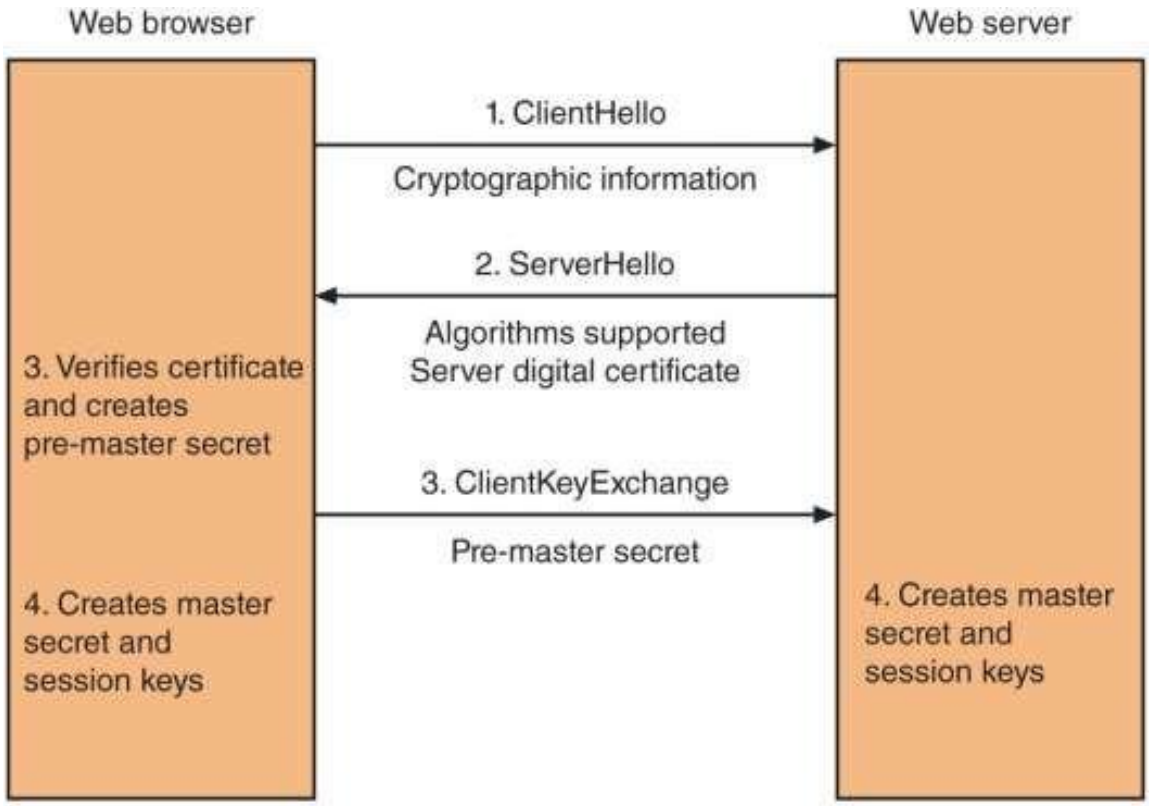


Figure 4-9 Key exchange

Domain Digital Certificates (3 of 5)

- **Domain validation** digital certificate
  - Verifies the identify of the entity that has control over the domain name

Figure 4-10 Domain validation padlock

Source: Google Chrome web browser

Domain Digital Certificates (4 of 5)

- **Extended Validation (EV)**
  - This type of certificate requires more extensive verification of the legitimacy of the business

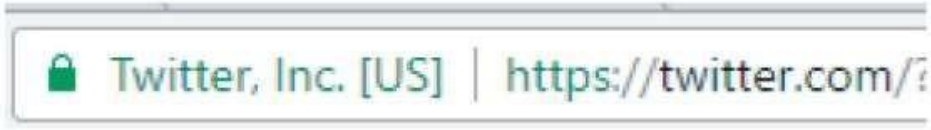


Figure 4-11 EV validation padlock

Source: Google Chrome web browser

Domain Digital Certificates (5 of 5)

- **Wildcard** digital certificate
  - Used to validate a main domain along with all subdomains
- **Subject Alternative Name (SAN)** digital certificate
  - Also known as a Unified Communications Certificate (UCC)
  - Primarily used for Microsoft Exchange servers or unified communications
- **Hardware and Software** digital certificates
  - **Machine digital certificate**
  - **Code signing digital certificate**
  - **Email digital certificate**

Digital Certificate Formats

- The most widely accepted digital certificates are defined by a division of the ITU
    - Known as the Telecommunication Standardization Sector (ITU-T)
- Adhere to the x.509 standard
- All x.509 certificates follow the standard ITU-T x.690, which specifies one of three encoding formats:
    - Basic Encoding Rules (BER)
    - Canonical Encoding Rules (CER)
    - Distinguished Encoding Rules (DER)

Public Key Infrastructure (PKI)

- Important management tool for the use of:
  - Digital certificates:
  - Asymmetric cryptography
- Important to understand PKI
  - How it is managed
  - How key management is performed
  - Know PKI trust models

What is Public Key Infrastructure (PKI)?

- There is a need for a consistent means to manage digital certificates
- **Public key infrastructure (PKI)** - a framework for all entities involved in digital certificates
- Certificate management actions facilitated by PKI
    - Create
    - Store
    - Distribute
    - Revoke

Trust Models

- **Trust**
  - Confidence in or reliance on another person or entity
- **Trust model**
  - Refers to the type of trust relationship that can exist between individuals and entities
- **Direct trust**
  - A type of trust model where one person knows the other person
- **Third-party trust**
  - Two individuals trust each other because each trusts a third party

Hierarchical Trust Model (1 of 3)

- 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
  - Can be used in an organization where one CA is responsible for only that organization's digital certificates

Hierarchical Trust Model (2 of 3)

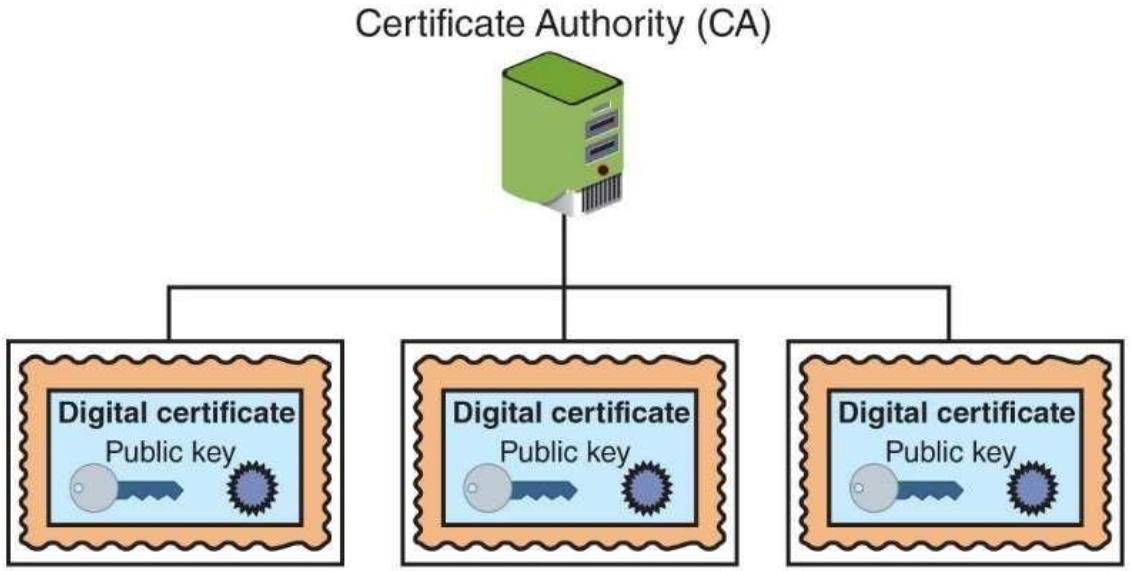


Figure 4-12 Hierarchical trust model

Hierarchical trust model limitations?

Hierarchical Trust Model (3 of 3)

- Hierarchical trust model limitations:
  - A single CA private key may be compromised rendering all certificates worthless
  - Having a single CA who must verify and sign all digital certificates may create a significant backlog (e.g., bottleneck)

Distributed Trust Model

- Distributed Trust Model
  - Multiple CAs sign digital certificates
  - Eliminates limitations of hierarchical trust model

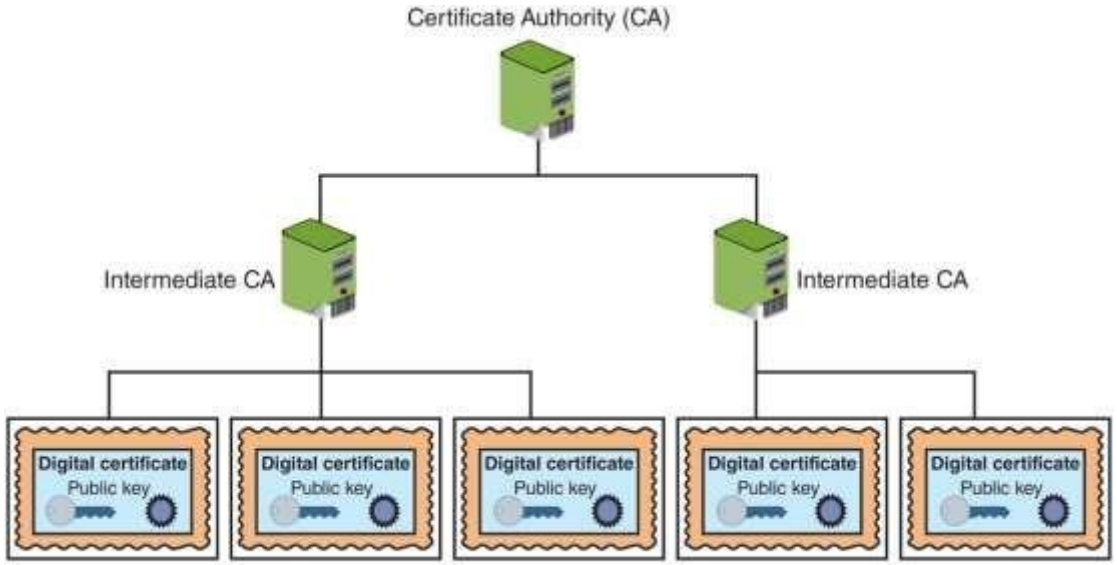


Figure 4-13 Distributed trust model

Bridge Trust Model (1 of 2)

- Bridge Trust Model
  - One CA acts as facilitator to interconnect connect all other CAs
  - Facilitator CA does not issue digital certificates, instead it acts as hub between hierarchical and distributed trust model
  - Allows the different models to be linked

Bridge Trust Model (2 of 2)

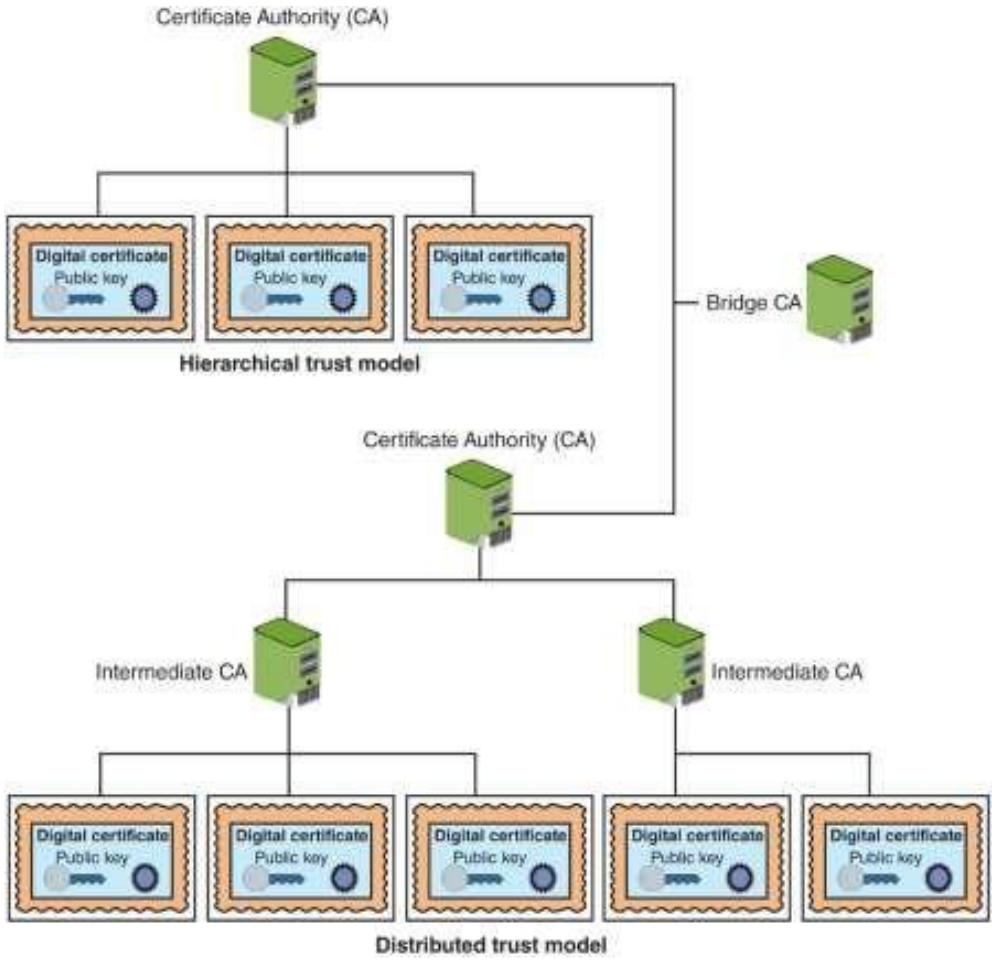


Figure 4-14 Bridge trust model

Managing PKI (1 of 2)

- **Certificate Policy (CP)**
  - A published set of rules that govern 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)**
  - A technical document that describes in detail how the CA uses and manages certificates
  - 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 (2 of 2)

- Certificate life cycle
  - **Creation**
    - Occurs after user is positively identified
  - **Suspension**
    - May occur when employee on leave of absence
  - **Revocation**
    - Certificate no longer valid
  - **Expiration**
    - Key can no longer be used

Key Management

- Key Management includes:
  - Key storage
  - Key usage
  - Key handling procedures

Key Storage

- Means of public key storage
    - Embedding within digital certificates
- Means of private key storage
    - Stored on user's local system
- Software-based storage may expose keys to attackers
- Alternative: storing keys in hardware
    - Smart-cards
    - Tokens

Key Usage

- Multiple pairs of dual keys can be created
  - If more security is needed than a single set of public/private keys
  - One pair used to encrypt information
    - Public key backed up in another location
  - Second pair used only for digital signatures
    - Public key in that pair would never be backed up

Key Handling Procedures (1 of 3)

- Key escrow
  - Keys are managed by a third party, such as a trusted CA
  - Private key is split and each half is encrypted
  - Two halves sent to third party, which stores each half in separate location
  - User can retrieve and combine two halves and use this new copy of private key for decryption
- Expiration
  - Keys expire after a set period of time
- Renewal
  - Existing key can be renewed

Key Handling Procedures (2 of 3)

- Revocation
  - Keys may be revoked prior to its expiration date
  - Revoked keys may not be reinstated
- Recovery
  - Need to recover keys of an employee hospitalized for extended period
  - Key recovery agent (KRA) may be used
  - Group of people may be used (M-of-N control)
- Suspension
  - Suspended for a set period of time and then reinstated
- Destruction
  - Removes all public and private keys and user's identification from the CA

Key Handling Procedures (3 of 3)

M-of-N control: requires the agreement of M out of a total of N authorized users to perform a specific action

Some common scenarios:

- **Bank transfer**: Two out of three bank managers need to approve a large money transfer before it can be processed
- **Safe unlocking**: Two separate keys held by different people are required to open a secure safe

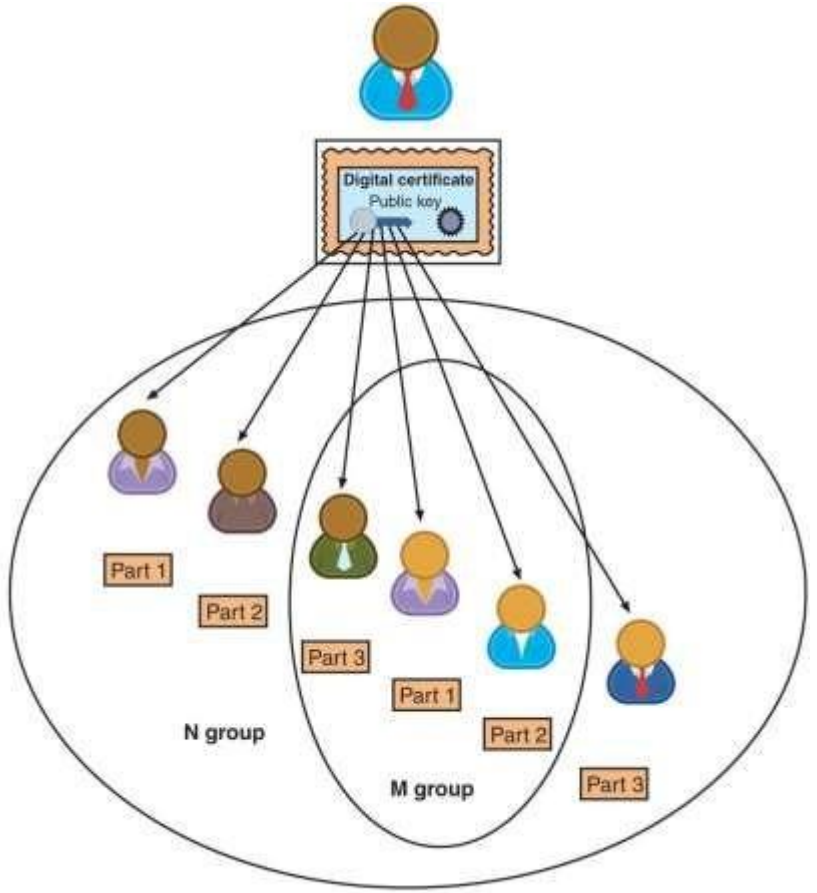


Figure 4-15 M-of-N control

Cryptographic Transport Protocols

- Most common cryptographic transport algorithms:
  - Secure Sockets Layer
  - Transport Layer Security
  - Secure Shell
  - Hypertext Transport Protocol Secure
  - S/MIME
  - Secure Real-time Transport Protocol
  - IP Security

Secure Sockets Layer (SSL)

- Secure Sockets Layer (SSL)
  - One of the most common transport algorithms
  - Developed by Netscape
  - Design goal was to create an encrypted data path between a client and a server
  - Uses the Advanced Encryption Standard (AES)
  - SSL version 3.0 is the current version

Transport Layer Security (TLS)

- Transport Layer Security (TLS)
  - SSL v3.0 served as the basis for TLS v1.0
  - Versions starting with v1.1 are significantly more secure than SSL v3.0
  - Current version is TLS v1.2
- **Cipher suite**
  - A named combination of the encryption, authentication, and message authentication code (MAC) algorithms that are used with SSL and TLS
- Length of keys - a factor in determining the overall security of a transmission
  - Keys of less than 2048 bits are considered weak
  - Keys of 2048 bits are considered good
  - Keys of 4096 bits are strong

Secure Shell (SSH)

- An encrypted alternative to the Telnet protocol used to access remote computers
- It is a Linux/UNIX-based command interface and protocol
- SSH is a suite of three utilities: slogin, ssh, and scp
- Client and server ends of the connection are authenticated using a digital certificate and passwords are encrypted
- Can be used as a tool for secure network backups

Hypertext Transport Protocol Secure (HTTPS)

- A common use of TLS and SSL:
  - To secure Hypertext Transport Protocol (HTTP) communications between browser and Web server
- The secure version is actually "**plain**" HTTP sent over SSL or TLS
- Called Hypertext Transport Protocol Secure (HTTPS) and uses port 443 instead of HTTP's port 80
- Users must enter URL s with https://

Secure/Multipurpose Internet Mail Extensions (S/MIME)

- Secure/Multipurpose Internet Mail Extensions (S/MIME)
    - A protocol for securing email messages
- Allows users to send encrypted messages that are also digitally signed

Secure Real-time Transport Protocol (SRTP)

- Secure Real-time Transport Protocol (SRTP)
    - A secure extension protecting transmission using the Real-time Transport Protocol (RTP)
- SRTP provides protection for Voice over IP (VoIP) communications
- Adds security features such as message authentication and confidentiality for VoIP Communications

IP Security (IPsec)

- 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
  - Key management
- Supports two encryption modes:
  - Transport - encrypts only the data portion of each packet and leaves the header unencrypted
  - Tunnel - encrypts both the header and the data portion

Chapter Summary (1 of 2)

- Cryptography that is improperly applied can lead to vulnerabilities that will be exploited
- A digital certificate is the user's public key that has been digitally signed by a trusted third party who verifies the owner and that the public key belongs to that owner
- A certificate repository (CR) is a list of approved digital certificates
- Revoked digital certificates are listed in a Certificate Revocation List (RCL)
    - Status can also be checked through the Online Certificate Status Protocol (OCSP)
- There are several different types of digital certificates

Chapter Summary (2 of 2)

- Domain validation digital certificates verify the identity of the entity that has control over the domain name but indicate nothing regarding the trustworthiness of the individuals behind the site
- A public key infrastructure (PKI) is a framework for all the entities involved in digital certificates to create, store, distribute, and revoke digital certificates
- An organization that uses multiple digital certificates on a regular basis needs to properly manage those digital certificates
- Cryptography is commonly used to protect data-in-transit
    - SSL and TLS are widely used protocols
- IPsec is a set of protocols developed to support the secure exchange of packets