Information Security (CP3404)

Chapter 6 – Advanced Cryptography

Based on the Fifth Edition of:

M. Ciampa:. *CompTIA® Security + Guide to Network Security Fundamentals*

Department of Information Technology, College of Business, Law & Governance

Learning Objectives

- Define digital certificates
- List various types of digital certificates and how they are used
- Describe components of Public Key Infrastructure (PKI)
- List tasks associated with key management
- Describe different transport encryption algorithms

Outline

Preface

- Cryptography has clear safeguarding sensitive data for end users (if everything goes well), i.e.,
  - Hasing ensures the integrity of a file
  - Symmetric encryption ensures Integrity and confidentiality of messages
  - Asymmetric encryption ensures authenticity, confidentiality, and nonrepudiation of messages
- But, there are some issues that need to be fixed

Digital Certificates

Digital Certificates

- One of the 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

Digital Certificates

Issues with Authentication

- Digital signatures – Used to prove document originated from valid sender, but
  - Do not confirm true identity of the sender
  - Digital signatures only show that private key of the sender was used to generate the digital signature
  - Do not definitively prove who the sender was
  - Imposter could post a public key under a sender's name (see Figure 6-1)

Digital Certificates

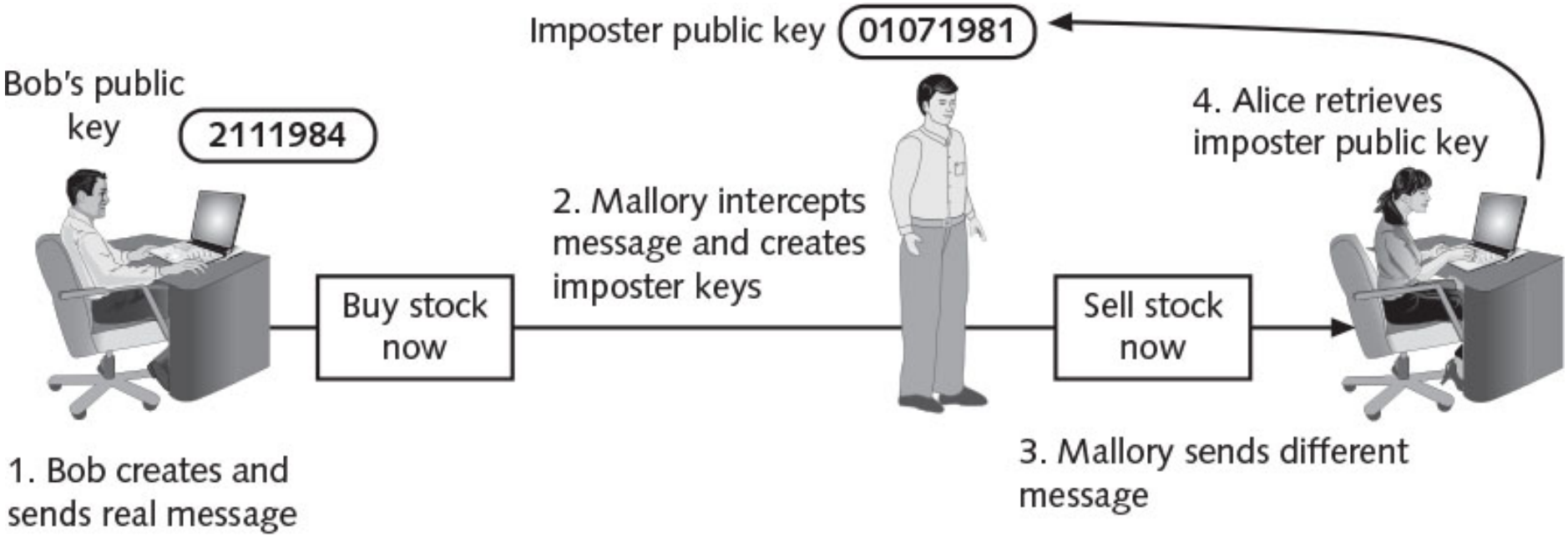

Figure 6-1 Imposter public key

Digital Certificates

Issues with Authentication

- Solution is use trusted third party
  - Used to address problem of verifying identity
  - Verifies owner and that public key belongs to that owner
  - Helps prevent man-in-the-middle attack that impersonates owner of public key

Digital Certificates

Digital Certificate

- Digital certificate – Technology used to associate user's identity to public key that has been digitally signed by a trusted third party
- Third party verifies owner and that public key belongs to that owner

Digital Certificates

Digital Certificate

- When Bob sends a message to Alice, he does not ask her to retrieve his public key from a central site
- Instead, Bob attaches digital certificate to message
- When Alice receives message with digital certificate, she can check the signature of trusted third party on certificate
- If signature was signed by a party that she trusts, then Alice can safely assume that the public key contained in the digital certificate is actually from Bob

Digital Certificates

Digital Certificate

- Information contained in digital certificate:
  - Owner's name or alias
  - Owner's public key
  - Issuer's name
  - Issuer's digital signature
  - Digital certificate's serial number
  - Expiration date of public key

Digital Certificates

Managing Digital Certificates

- Entities and technologies used for managing digital certificates include
  - Certificate Authority (CA)
  - Registration Authority (RA)
  - Certificate Repository (CR)
  - Means to revoke certificate

Digital Certificates

Certificate Authority (CA)

- Certificate Authority (CA) – Trusted third-party agency responsible for issuing digital certificates
- CA can be:
  - External to organization, such as a commercial CA that charges for the service
  - Internal to organization that provides this service to employees

Digital Certificates

Duties of Certificate Authority (CA)

- Generate, issue, an distribute public key certificates
- Distribute CA certificates
- Generate and publish certificate status information
- Provide a means for subscribers to request revocation
- Revoke public-key certificates
- Maintain security, availability, and continuity of certificate issuance signing functions

Digital Certificates

Steps for Requesting Digital Certificate

- Generate public and private keys
- Generate Certificate Signing Request (CSR) – Specially formatted encrypted message that validates information CA requires (see Table 6-1)
- CA receives and verifies the CSR
- Inserts the public key into certificate
- Certificates digitally signed with private key of the issuing CA

Because digital certificates are used extensively on the Internet, web browsers are preconfigured with a default list of CAs (see Figure 6-2)

Digital Certificates

Name	Description	Example
Common name	Fully qualified domain name (FQDN) of the server	www.acompany.net
Business name	Legal name of organization	A Company, Inc.
Department	Division of the organization	Information Technology
City	City of the organization	Tampa
State	State of the organization	FL
Country	Two-letter code of country	US
Email address	Address of contact person	cio@acompany.net

Table 6-1 Certificate Signing Request content

Digital Certificates

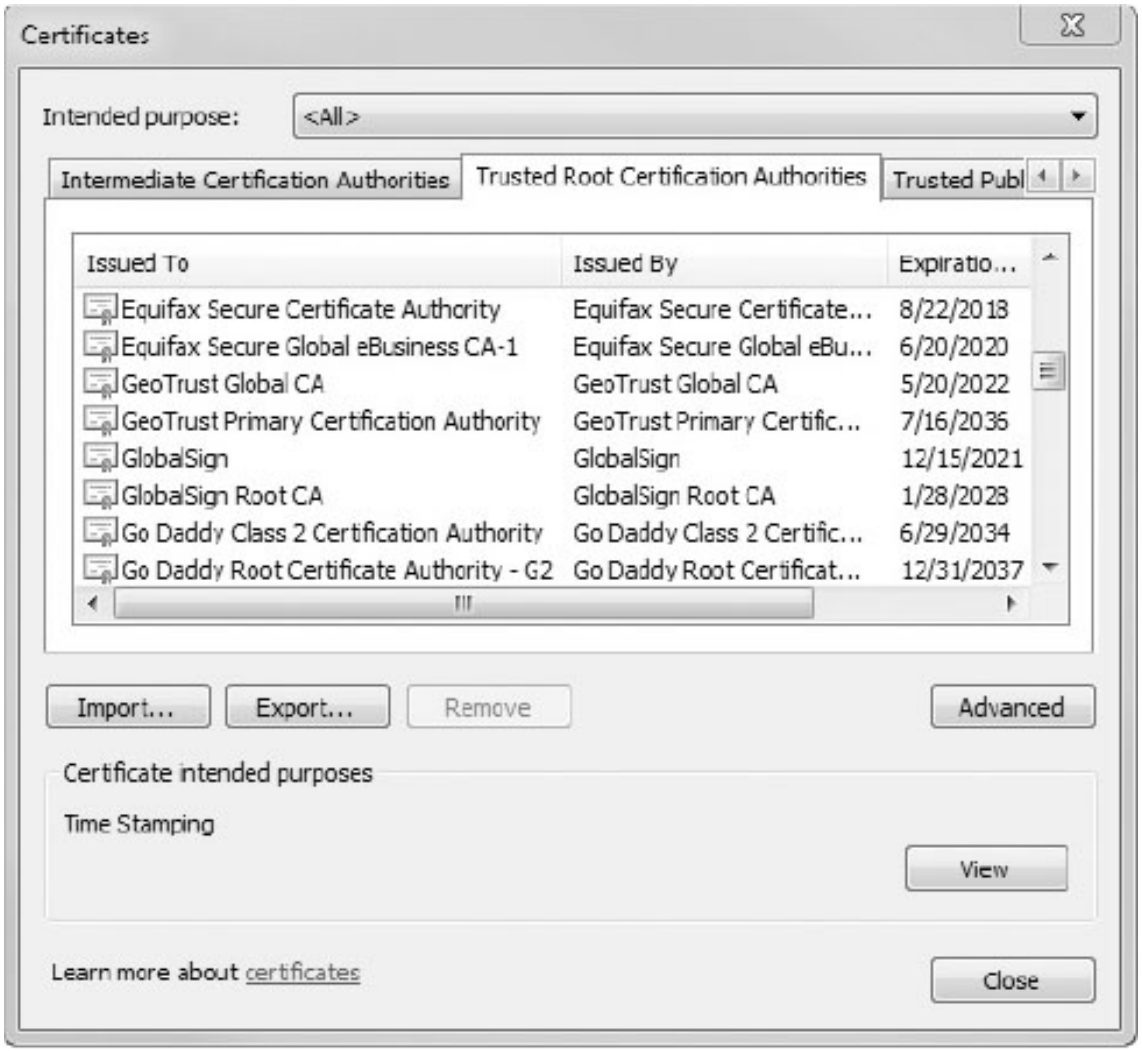

Figure 6-2 Web browser default CAs

Source: Google Chrome web browser

Digital Certificates

Registration Authority (RA)

- Registration Authority – Subordinate entity designed to handle specific CA tasks (e.g., processing certificate requests, authenticating users)
- Using RAs (also called Local Registration Authorities or LRAs) can *off-load* registration functions and create an improved workflow

Digital Certificates

General Duties of Registration Authority (RA)

- Receive, authenticate, and process certificate revocation requests
- Identify and authenticate subscribers
- Obtain a public key from the subscriber
- Verify that subscriber possesses asymmetric private key corresponding to public key submitted for certification

Digital Certificates

General Duties of Registration Authority (RA)

- Primary function of RA is verify identity individual
- Different means for a digital certificate requester to identify themselves to RA:
  - E-mail – Insufficient for activities that must be very secure
  - Documents – Birth certificate, employee badge
  - In person – Providing government-issued passport or driver's license

Digital Certificates

Certificate Repository (CR)

- Certificate Repository (CR) – Publicly accessible centralized directory of digital certificates
- Used to view certificate status
- Can be managed locally as a storage area connected to the CA server

Digital Certificates

Certificate Revocation

- Digital certificates normally have an expiration date (one year from date issued)
- Circumstances that may be cause for certificate to be revoked before expires:
  - Certificate no longer used
  - Details of certificate changed
  - Someone steal a user's private key (impersonate victim through using digital certificates)
  - Digital certificates stolen from CA

Digital Certificates

Certificate Revocation List (CRL)

- Current status of certificate can be checked to determine if has been revoked
- Certificate Revocation List (CRL) – Serves as list of certificate serial numbers that have been revoked
- Many CAs maintain an online CRL that can be queried by entering the certificate's serial number
- Local computer receives updates on the status of certificates and maintains a local CRL (see Figure 6-3)

Digital Certificates

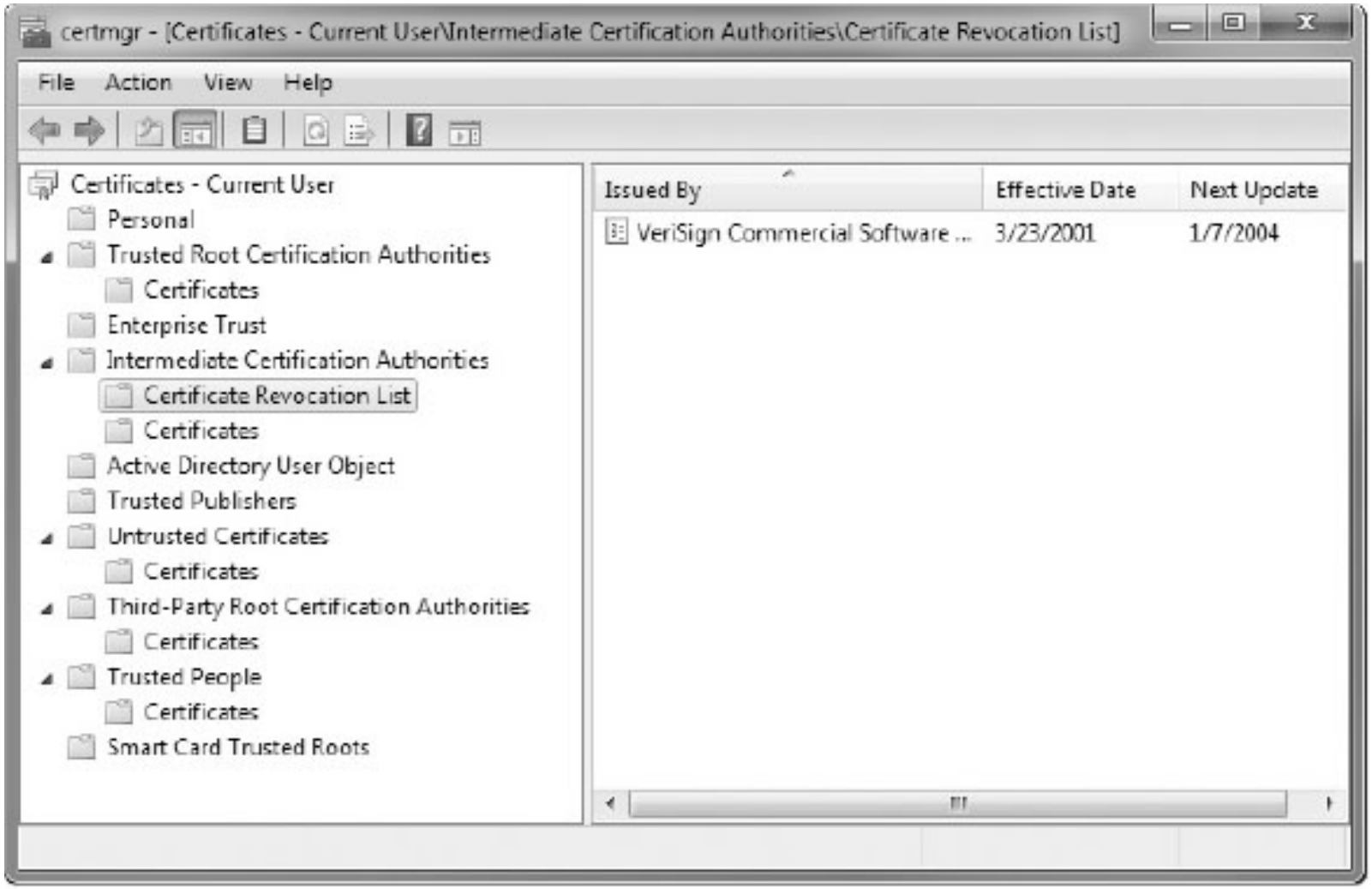

Figure 6-3 Certificate Revocation List (CRL)

Source: Microsoft Windows

Digital Certificates

Online Certificate Status Protocol (OCSP)

- OCSP Performs real-time lookup of a certificate's status
- Browser sends certificate's information to a trusted entity like the CA, known as an OCSP Responder
- OCSP stapling is a variation of OCSP
- When Web browser attempts to connect to web server the server can include (staple) in handshake previously received OCSP response (see Figure 6-4)

Digital Certificates

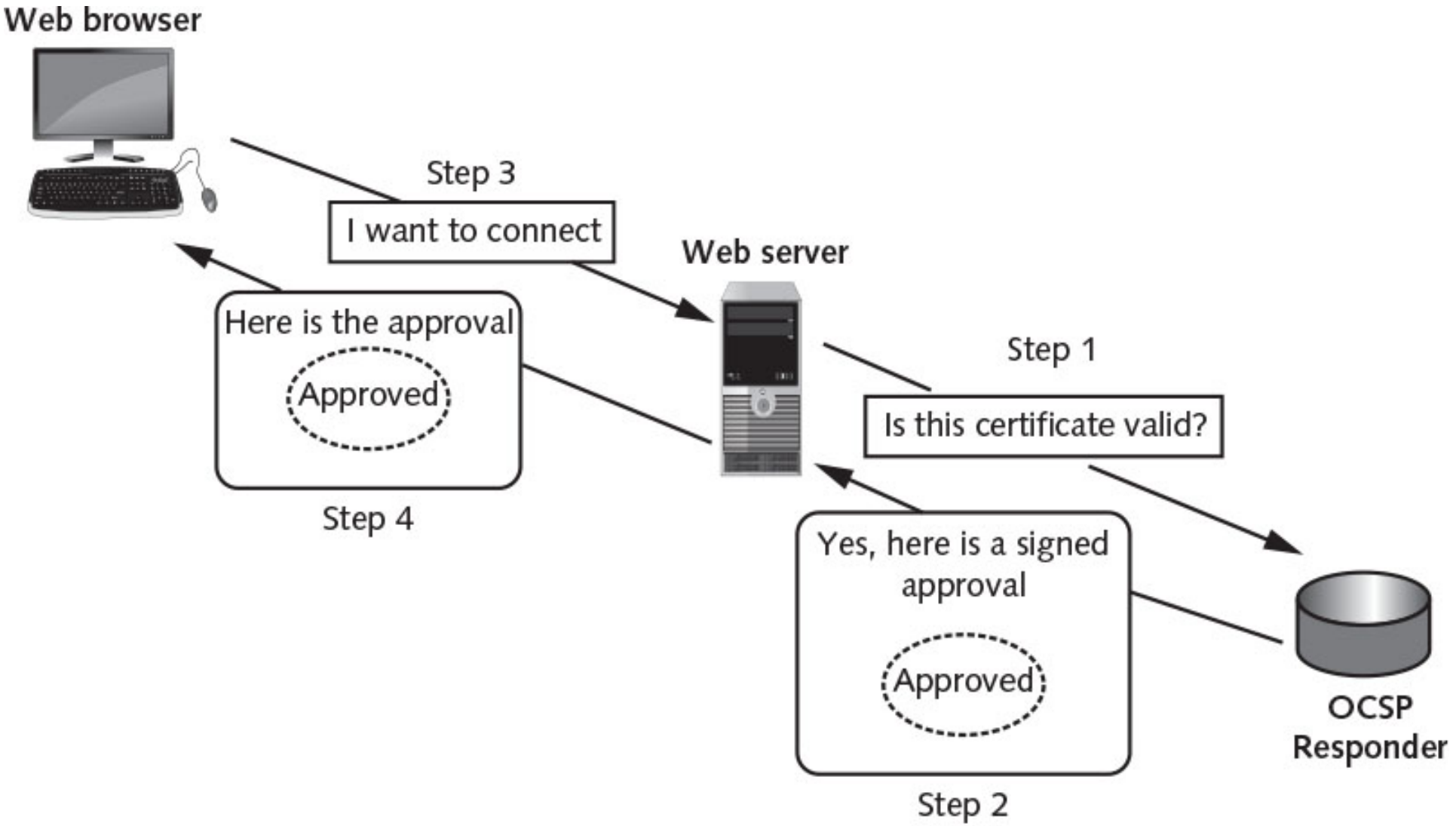

Figure 6-4 OCSP stapling

Digital Certificates

Types of Digital Certificates

- There are different categories of digital certificates; most common categories are:
  - Personal Digital Certificates (Class 1)
  - Server Digital certificates (Class 2)
  - Software Publisher Digital certificates (Class 3)

Note that Class 4 and Class 5 are specialized digital certificates (for online business transactions, and private organizations or governmental security, respectively)

Digital Certificates

Personal Digital Certificates

- Personal digital certificates (Class 1) – Issued by RA directly to individuals
- Frequently used to secure email transmissions
- Typically require only user's name and email address in order to receive this certificate
- Can also be used to authenticate the authors of documents
- User can create Microsoft Word or Adobe Portable Document Format (PDF) document and then use digital certificate to create digital signature

Digital Certificates

Server Digital Certificates

- Server digital certificates (Class 2) – Often issued from web server to client, and perform two (2) functions:
  1. Can ensure the authenticity of the web server
  2. Can ensure the authenticity of the cryptographic connection to the web server
- Web servers set up secure cryptographic handshake connections so that all transmitted data is encrypted by providing server's public key with digital certificate to client (see Figure 6-5)

Digital Certificates

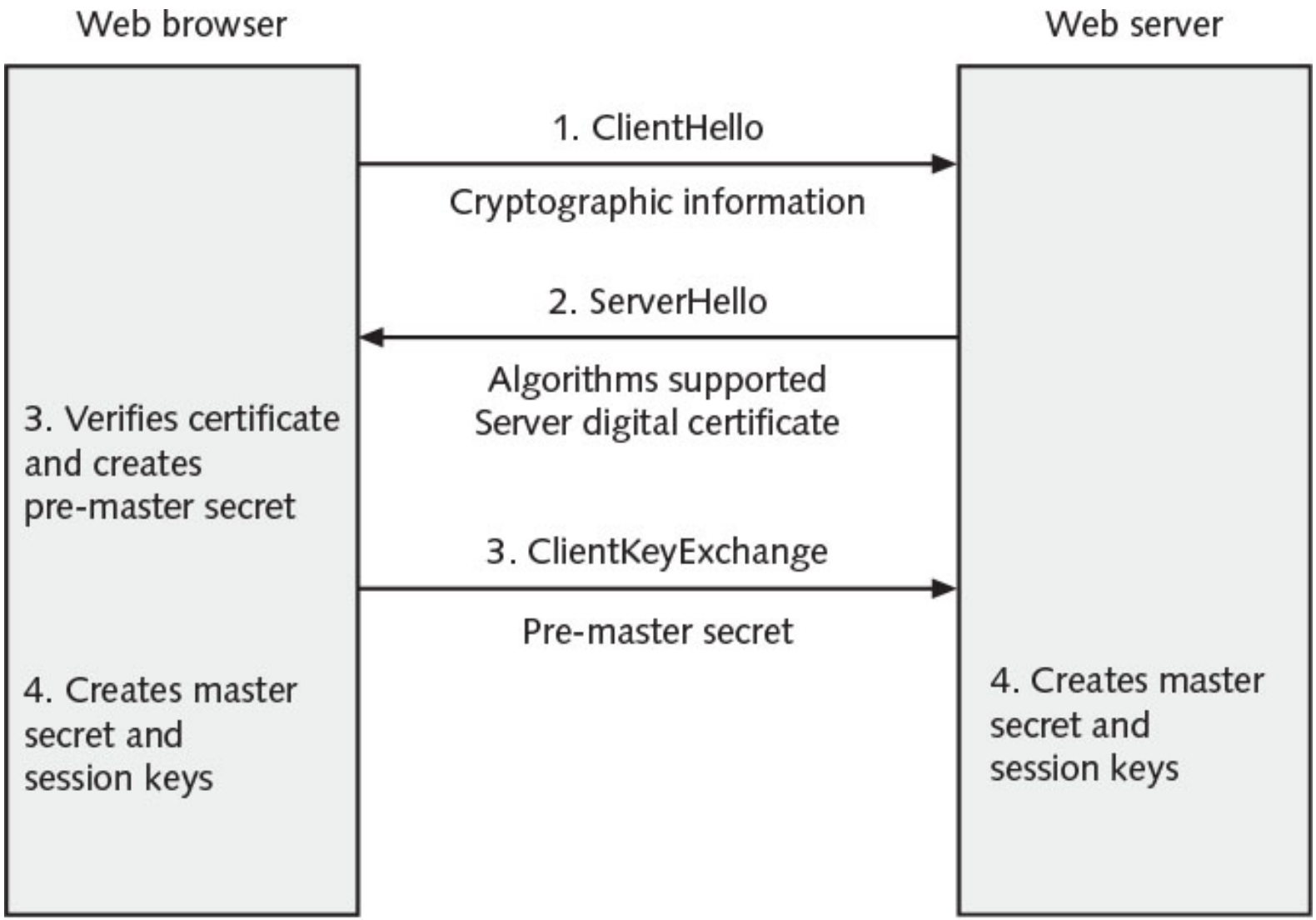

Figure 6-5 Server digital certificate handshake

Digital Certificates

Server Digital Certificates (Cont.)

- Server digital certificate that both verifies existence and identity of the organization and securely encrypts communications displays a padlock icon in the web browser (see Figure 6-6)
- Clicking padlock icon displays information about digital certificate along with the name of the site
- Extended Validation SSL Certificate (EV SSL) – Enhanced type of server digital certificate that requires more extensive verification of legitimacy of the business

Digital Certificates

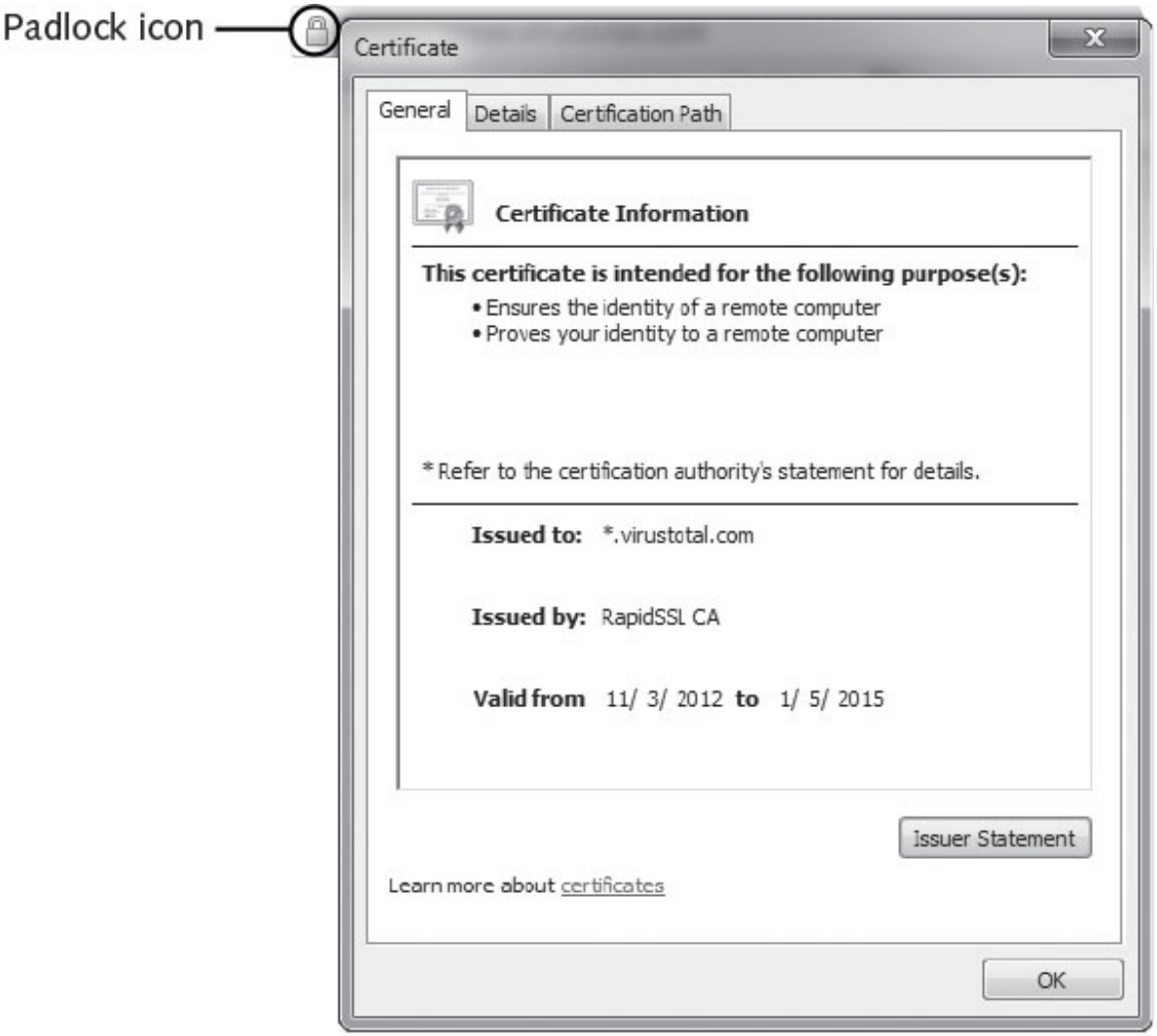

Figure 6-6 Padlock icon and certificate information

Source: Google Chrome web browser

Digital Certificates

Software Publisher Digital Certificates

- Software publisher digital certificates (Class 3) – Provided by software publishers
- Purpose to verify that their programs are secure and have not been tampered with
- Remaining two classes of digital certificates are specialized:
  - Class 4 is for online business transactions between companies
  - Class 5 is for private organizations or governmental security

Digital Certificates

X.509 Digital Certificate

- The most widely accepted format for digital certificate is defined by the International Telecommunication Union (ITU), i.e., X.509 international standard
- Digital certificates following this standard can be read or written by any application that follows X.509
- The current version is X.509 v3 (see Table 6-2)

Digital Certificates

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

Table 6-2 X.509 structure

Quick Quiz

1. _____ can be used to associate or *bind* a user's identity to a public key.
   Answer:

Quick Quiz

1. _____ can be used to associate or *bind* a user's identity to a public key.
   Answer: Digital certificates

Quick Quiz

1. _____ can be used to associate or *bind* a user's identity to a public key.
   Answer: Digital certificates

2. A specially formatted encrypted message that validates the information the CA requires to issue a digital certificate is known as a(n) _____.
   answer:

Quick Quiz

1. _____ can be used to associate or *bind* a user's identity to a public key.
   Answer: Digital certificates

2. A specially formatted encrypted message that validates the information the CA requires to issue a digital certificate is known as a(n) _____.
   answer: Certificate Signing Request (CSR)

Quick Quiz

1. _____ can be used to associate or *bind* a user's identity to a public key.
   Answer: Digital certificates

2. A specially formatted encrypted message that validates the information the CA requires to issue a digital certificate is known as a(n) _____.
   answer: Certificate Signing Request (CSR)

3. Revoked digital certificates are listed in a(n) _____, which can be accessed to check the certificate status of other users.
   Answer:

Quick Quiz

1. _____ can be used to associate or *bind* a user's identity to a public key.
   Answer: Digital certificates

2. A specially formatted encrypted message that validates the information the CA requires to issue a digital certificate is known as a(n) _____.
   answer: Certificate Signing Request (CSR)

3. Revoked digital certificates are listed in a(n) _____, which can be accessed to check the certificate status of other users.
   Answer: Certificate Revocation List (CRL)

Quick Quiz

1. _____ can be used to associate or *bind* a user's identity to a public key.
   Answer: Digital certificates

2. A specially formatted encrypted message that validates the information the CA requires to issue a digital certificate is known as a(n) _____.
   answer: Certificate Signing Request (CSR)

3. Revoked digital certificates are listed in a(n) _____, which can be accessed to check the certificate status of other users.
   Answer: Certificate Revocation List (CRL)

4. The master secret is used to create _____, which are symmetric keys to encrypt and decrypt information exchanged during the session and to verify its integrity.
   Answer:

Quick Quiz

1. _____ can be used to associate or *bind* a user's identity to a public key.
   Answer: Digital certificates

2. A specially formatted encrypted message that validates the information the CA requires to issue a digital certificate is known as a(n) _____.
   answer: Certificate Signing Request (CSR)

3. Revoked digital certificates are listed in a(n) _____, which can be accessed to check the certificate status of other users.
   Answer: Certificate Revocation List (CRL)

4. The master secret is used to create _____, which are symmetric keys to encrypt and decrypt information exchanged during the session and to verify its integrity.
   Answer: session keys

Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI)

- Public key infrastructure (PKI) – Underlying infrastructure for management of public keys used in digital certificates
- PKI is framework for all of entities (hardware, software, people, policies and procedures) involved in digital certificates for digital certificate management to create, store, distribute, and revoke digital certificates

Public Key Infrastructure (PKI)

Public Key Cryptography Standards (PKCS)

- Public key cryptography standards (PKCS) – Numbered set of PKI standards that been defined by RSA Corporation
- Although informal standards, today widely accepted in industry
- PKCS is composed of 15 standards (see Table 6-3)
- Applications and products that are developed by vendors may choose to support the PKCS (See Figure 6-7)

Public Key Infrastructure (PKI)

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	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	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 (PBE) Standard
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
PKCS #11	2.20	Cryptographic Token Interface Standard	Defines a technology-independent device interface, called Cryptoki, that is used for security tokens, such as smart cards
PKCS #12	1.0	Personal Information Exchange Syntax Standard	Defines the file format for storing and transporting a user's private keys with a public key certificate
PKCS #13	Under development	Elliptic Curve Cryptography Standard	Defines the elliptic curve cryptography algorithm for use in PKI; describes mechanisms for encrypting and signing data using elliptic curve cryptography
PKCS #14	Under development	Pseudorandom Number Generation Standard	Covers pseudorandom number generation (PRNG)
PKCS #15	1.1	Cryptographic Token Information Format Standard	Defines a standard for storing information on security tokens

Table 6-3 PKCS standards

Public Key Infrastructure (PKI)

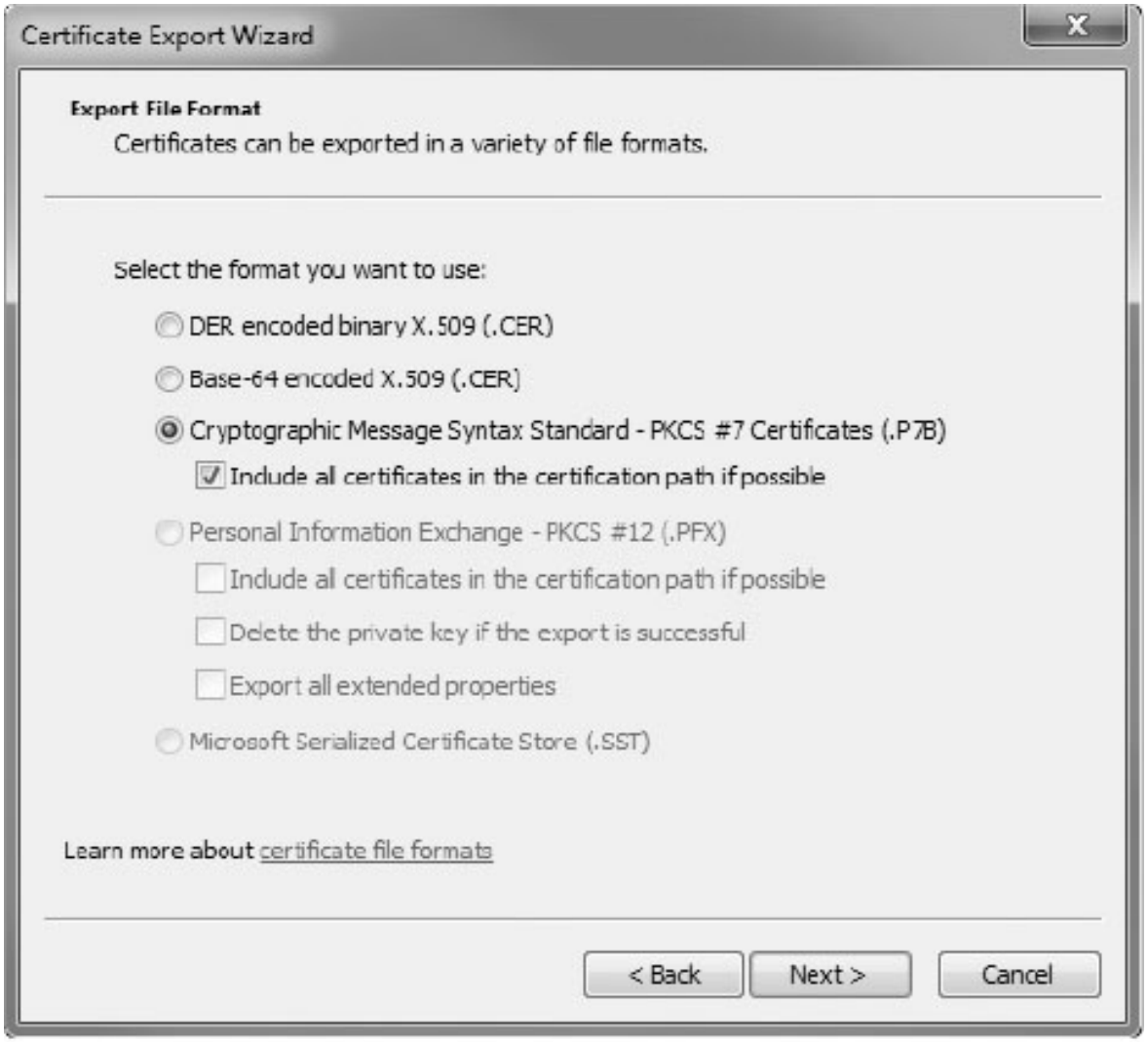

Figure 6-7 Microsoft Windows PKCS support

Source: Microsoft Windows

Public Key Infrastructure (PKI)

Trust Models

- Trust – Confidence in or reliance on another person or entity
- Trust model – Refers to type of trusting relationship that can exist between individuals and entities
  - Direct trust – One person knows the other person
  - Third-party trust – Two individuals trust each other because each trusts a third party
- Three (3) PKI trust models use a CA
  1. Hierarchical trust Model
  2. Distributed Trust Model
  3. Bridge Trust Model

Public Key Infrastructure (PKI)

Hierarchical Trust Model

- Hierarchical trust model – Assigns single hierarchy with one master CA called the root (see Figure 6-8)
- Root signs all digital certificate authorities with single key
- Can be used in organization where one CA is responsible for only that organization's digital certificates
- Hierarchical trust model has limitations: Single CA private key may be compromised rendering all certificates worthless

Public Key Infrastructure (PKI)

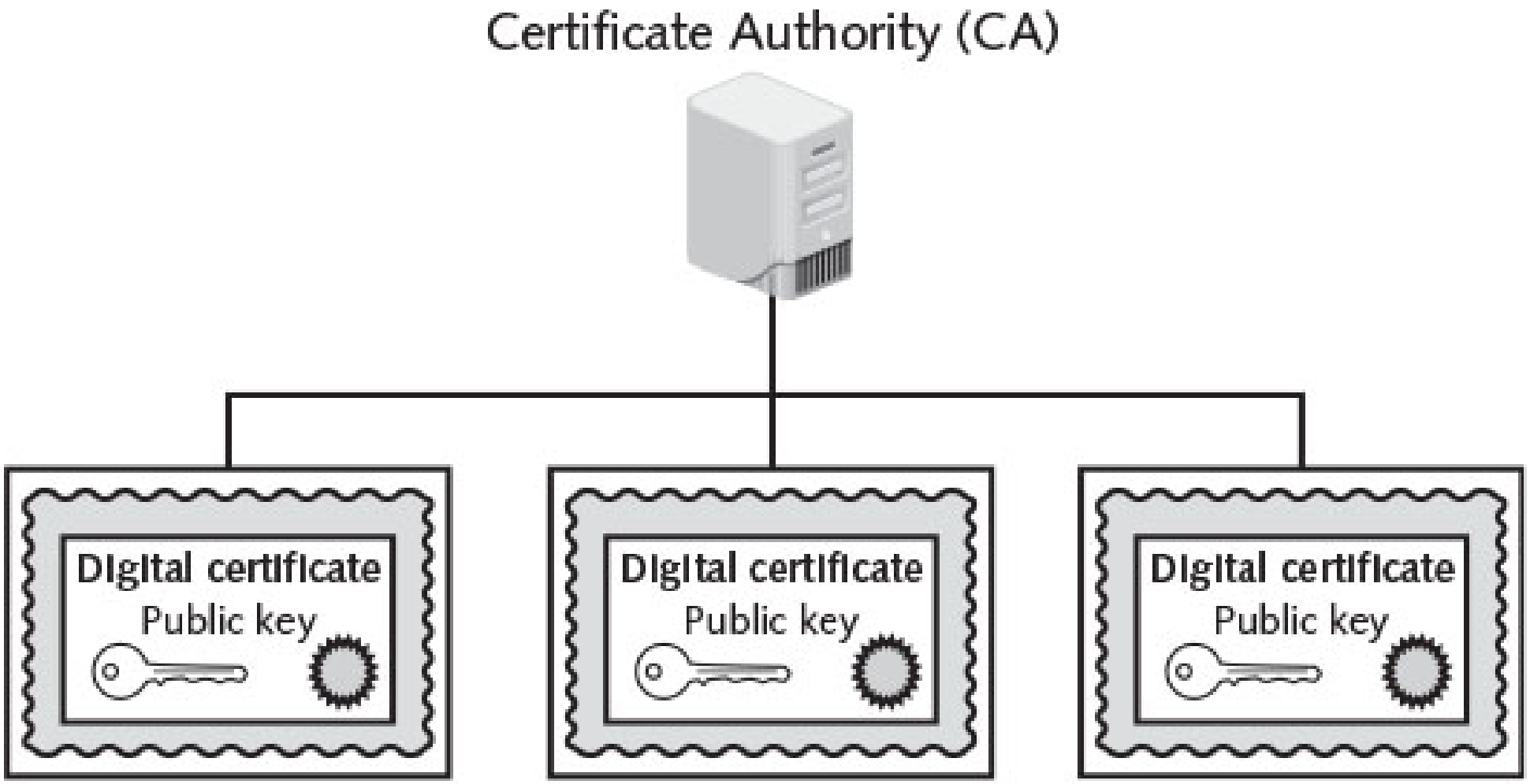

Figure 6-8 Hierarchical trust model

Public Key Infrastructure (PKI)

Distributed Trust Model

- Multiple CAs sign digital certificates (see Figure 6-9)
- Eliminates limitations of hierarchical trust model
- Basis for most end-user digital certificates used on the Internet (see Figures 6-2 and 6-3)
  - Trusted root certification authorities
  - Intermediate certification authorities
- Allows chain to be established: web browser trusts the intermediate CA because the certificate was issued through a higher-level trusted root CA that it trusts

Public Key Infrastructure (PKI)

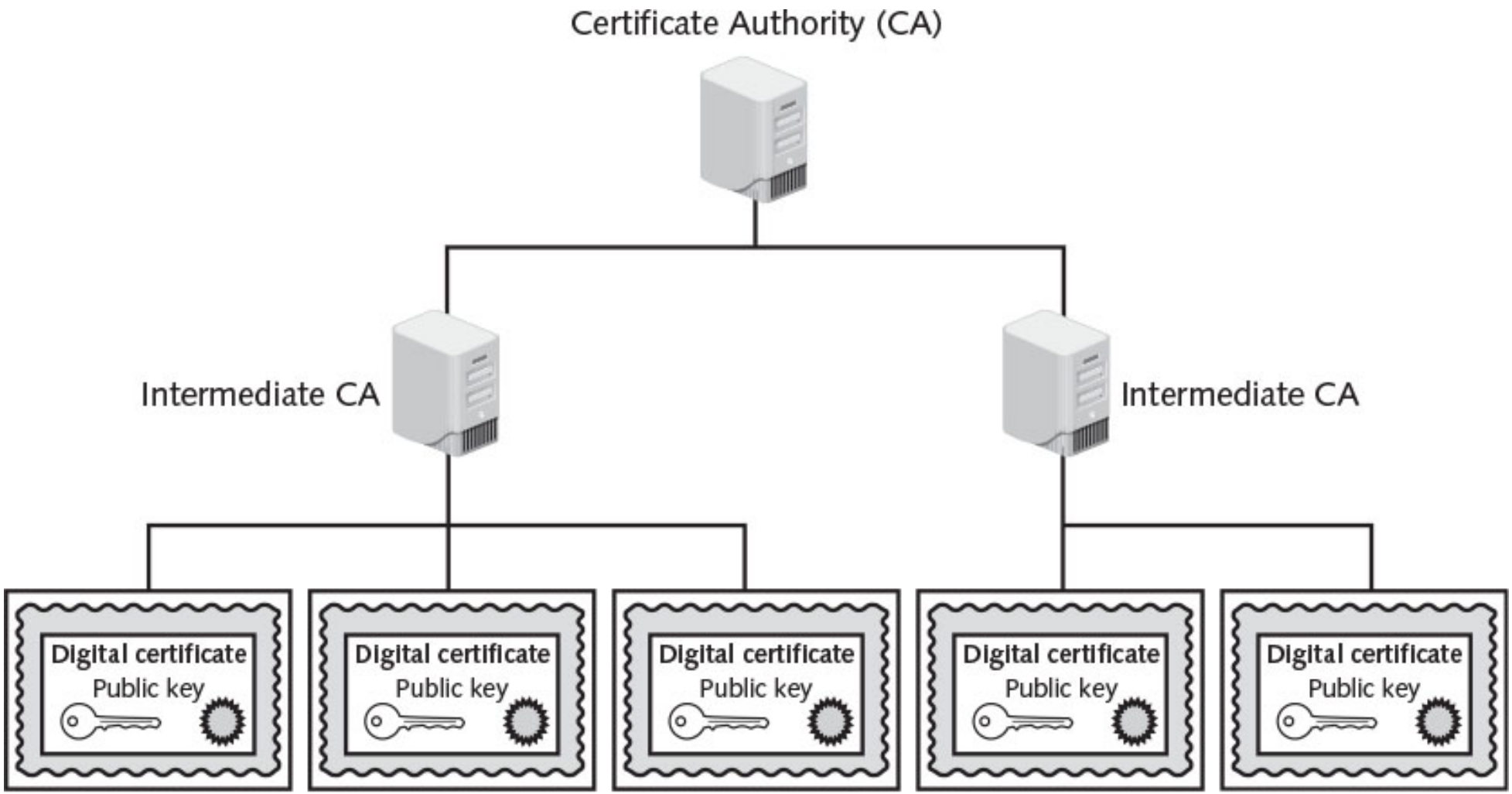

Figure 6-9 Distributed trust model

Public Key Infrastructure (PKI)

Bridge Trust Model

- Bridge trust model – One CA acts as facilitator to connect all other CAs
- Acts as hub between hierarchical and distributed trust model
- Allows the different models to be linked (see Figure 6-10)

Public Key Infrastructure (PKI)

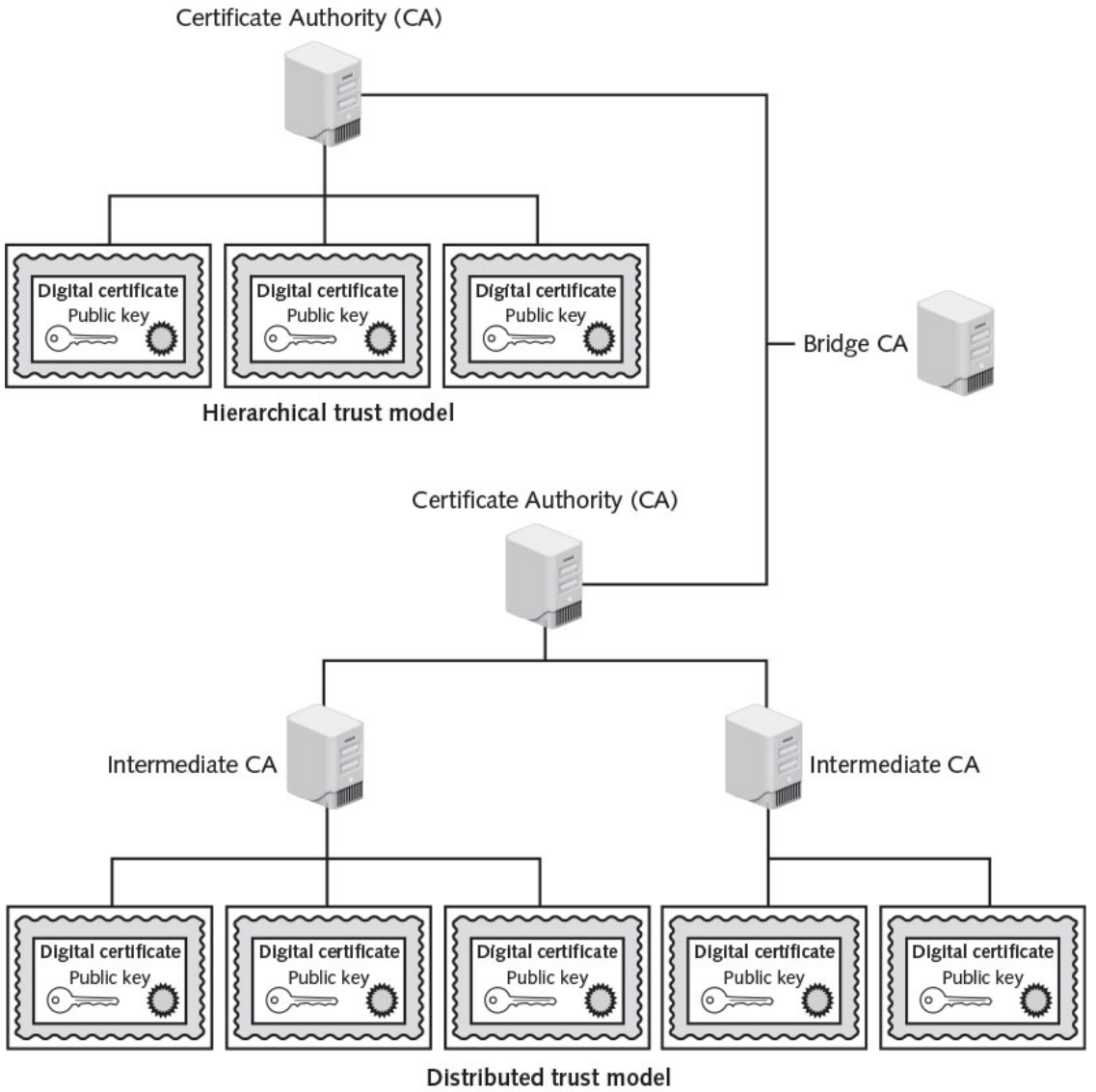

Figure 6-10 Bridge trust model

Public Key Infrastructure (PKI)

Managing PKI

- Certificate Policy (CP) – Published set of rules that govern operation of a PKI
- Provides recommended baseline security requirements for use and operation of CA, RA, and other PKI components
- Certificate Practice Statement (CPS) – Describes in detail how the CA uses and manages certificates

Public Key Infrastructure (PKI)

Certificate Life Cycle

- Certificate life cycle divided into four (4) parts:
  1. Creation – Occurs after user is positively identified
  2. Suspension – May occur when employee on leave of absence
  3. Revocation – Certificate no longer valid
  4. Expiration – Key can no longer be used

Key Management

Key Management

- Because keys form the foundation of PKI systems, it is important that they be carefully managed
- Proper key management includes:
  - Key Storage
  - Key Usage
  - Key Handling Procedures

Key Management

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 is storing keys in hardware:
  - Tokens
  - Smart-cards

Key Management

Key Usage

- Multiple pairs of dual keys created if more security needed than 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 never backed up)

Key Management

Key Handling Procedures

- Certain procedures can help ensure that keys are properly handled
- Key handling procedures include:
  - Key Escrow
  - Key Expiration
  - Key revocation
  - Key recovery
  - Key Suspension
  - Key Destruction

Key Management

Key Handling Procedures — Key Escrow

- Key Escrow – Process in which keys are managed by a third party (like 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

Key Management

Key Handling Procedures — Key Expiration

- Keys expire after a set period of time
- Prevents attacker who may have stolen a private key from being able to decrypt messages for an indefinite period of time
- Some systems set keys to expire after set period of time by default

Key Management

Key Handling Procedures — Key Renewal

- Existing key can be renewed
- Continually renewing keys make them more vulnerable to theft or misuse

Key Handling Procedures — Key Revocation

- Key may be revoked prior to its expiration date
- Revoked keys may not be reinstated

Key Management

Key Handling Procedures — Key Recovery

- Need to recover keys of an employee hospitalized for extended period
- Key recovery agent (who is a highly trusted person) may be designated
- Group of people may be used (M-of-N control) —see Figure 6-11

Key Management

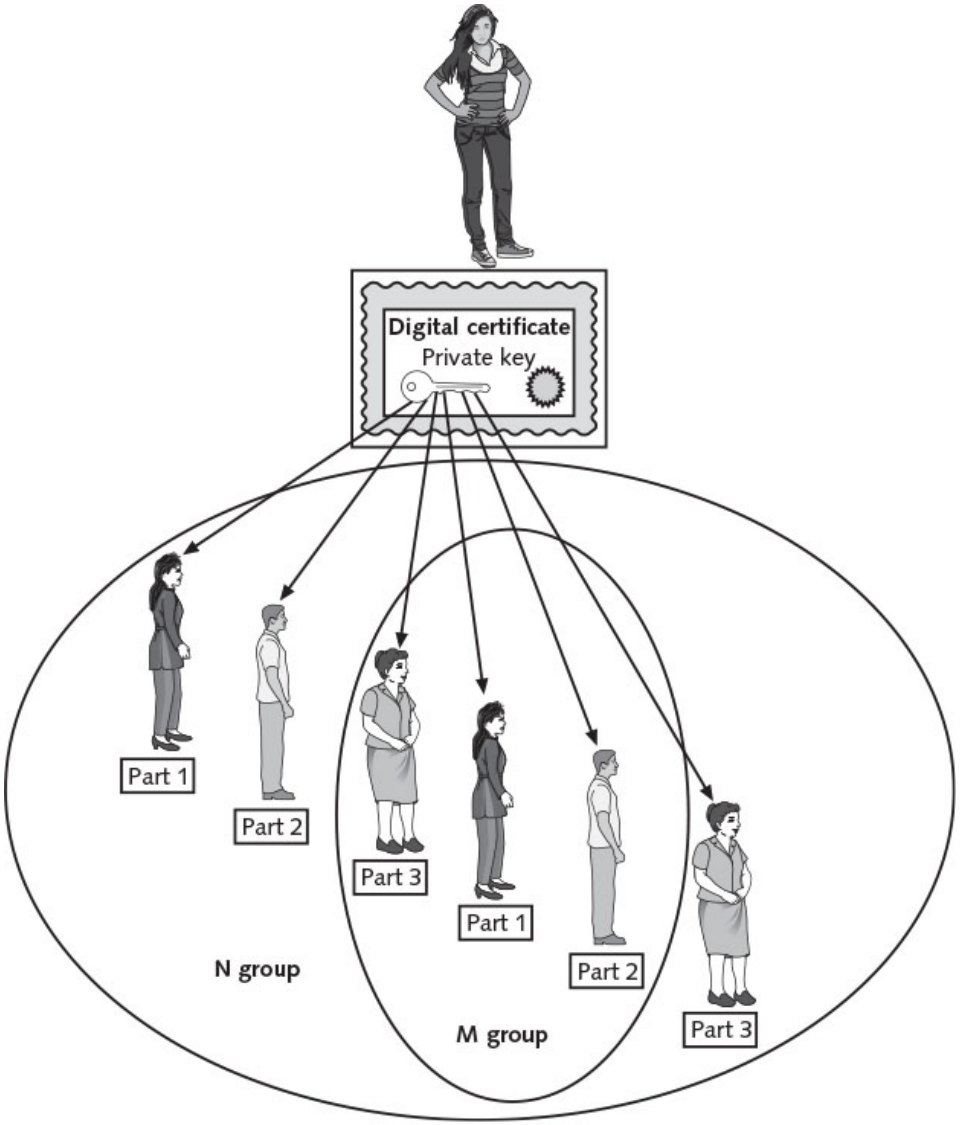

Figure 6-11 M-of-N control

Key Management

Key Handling Procedures — Key Suspension

- Suspended for a set period of time and then reinstated
- As with revocation, the CA should update CRL to verify that the key is no longer valid

Key Handling Procedures — Key Destruction

- Removes all public and private keys and user's identification from the CA
- User's information remains on the CA for audit purpose

Cryptographic Transport Protocols

Cryptographic Transport Protocols

- In addition to protecting data in-use and data at-rest, cryptography often used to protect data in-transit across network
- Most common cryptographic transport algorithms include
  - Secure Sockets Layer (SSL)
  - Transport Layer Security (TLS)
  - Secure Shell (SSH)
  - Hypertext Transport Protocol Secure (HTTPS)
  - IP Security (IPsec)

Cryptographic Transport Protocols

Secure Sockets Layer (SSL)

- Secure Sockets Layer (SSL) – One of most common transport encryption algorithm
- Developed by Netscape in 1994
- Uses AES (instead of DES) to encrypt data transferred over the SSL connection
- Today SSL version 3.0 is version most web servers support

Cryptographic Transport Protocols

Transport Layer Security (TLS)

- Although SSL and TLS are often used interchangeably or in conjunction with each other (TLS/SSL), this is incorrect:
  - SSL v3.0 served as the basis for TLS v1.0 (and is sometimes erroneously called SSL 3.1)
  - Versions of TLS (v1.1 and v1.2) are significantly more secure and address several vulnerabilities present in SSL v3.0 and TLS v1.0
  - Older and less secure versions still supported (see Table 6-4)

Cryptographic Transport Protocols

Protocol supported	Percentage of websites	Protocol security strength
SSL v2.0	23.0	Should not be used
SSL v3.0	99.3	Considered obsolete
TLS v1.0	97.7	Must be carefully configured
TLS v1.1	29.6	No known vulnerabilities
TLS v1.2	32.3	No known vulnerabilities

Table 6-4 Website support of SSL and TLS

Cryptographic Transport Protocols

Transport Layer Security (TLS) —Cipher Suite

- Depending on different algorithms that are selected, the overall security of the transmission may be either strong or weak
- Cipher Suite – Named combination of encryption, authentication, and message authentication code (MAC) algorithms used with SSL and TLS
- These negotiated between web browser and web server during the initial connection handshake

Cryptographic Transport Protocols

Secure Shell (SSH)

- Secure Shell (SSH) – Encrypted alternative to Telnet protocol used to access remote computers
- Linux/UNIX-based command interface and protocol
- Suite of three utilities: slogin, ssh, and scp (see Table 6-5)
- Client and server ends of connection are authenticated using a digital certificate
- Passwords are encrypted
- Can be used as a tool for secure network backups

Cryptographic Transport Protocols

UNIX command name	Description	Syntax	Secure command replacement
rlogin	Log on to remote computer	rlogin *remotecomputer*	slogin
rcp	Copy files between remote computers	rcp [*options*] *localfile remotecomputer:filename*	scp
rsh	Executing commands on a remote host without logging on	rsh *remotecomputer command*	ssh

Table 6-5 SSH commands

Cryptographic Transport Protocols

Hypertext Transport Protocol Secure (HTTPS)

- Common use of SSL and TLS is to secure Web Hypertext Transport Protocol (HTTP) communications between browser and web server
- Users must enter URLs with https:// instead of http://
- Uses port 443 instead of HTTP's port 80
- Secure Hypertext Transport Protocol (SHTTP) – Considered obsolete

Cryptographic Transport Protocols

IP Security (IPsec)

- Internet Protocol Security (IPsec) – Protocol suite for security Internet Protocol (IP) communications
- Encrypts and authenticates each IP packet of a session between hosts or networks
- Can provide protection to a much wider range of applications than SSL or TLS

Cryptographic Transport Protocols

IP Security (IPsec) —Cont.

- IPsec considered to be transparent security protocol to:
  - Applications – Programs do not have to be modified to run under IPsec
  - Users – Unlike some security tools, users do not need to be trained on specific security procedures (such as encrypting with PGP)
  - Software – Because IPsec is implemented in a device such as a firewall or router, no software changes must be made on the local client

Cryptographic Transport Protocols

IP Security (IPsec) —Cont.

- Located in operating system or communication hardware
- Provides authentication, confidentiality, and key management
- Supports two (2) encryption modes:
  1. Transport mode – Encrypts only the data portion (payload) of each packet yet leaves the header unencrypted
  2. Tunnel mode – Encrypts both the header and the data portion (see Figure 6-12)

Cryptographic Transport Protocols

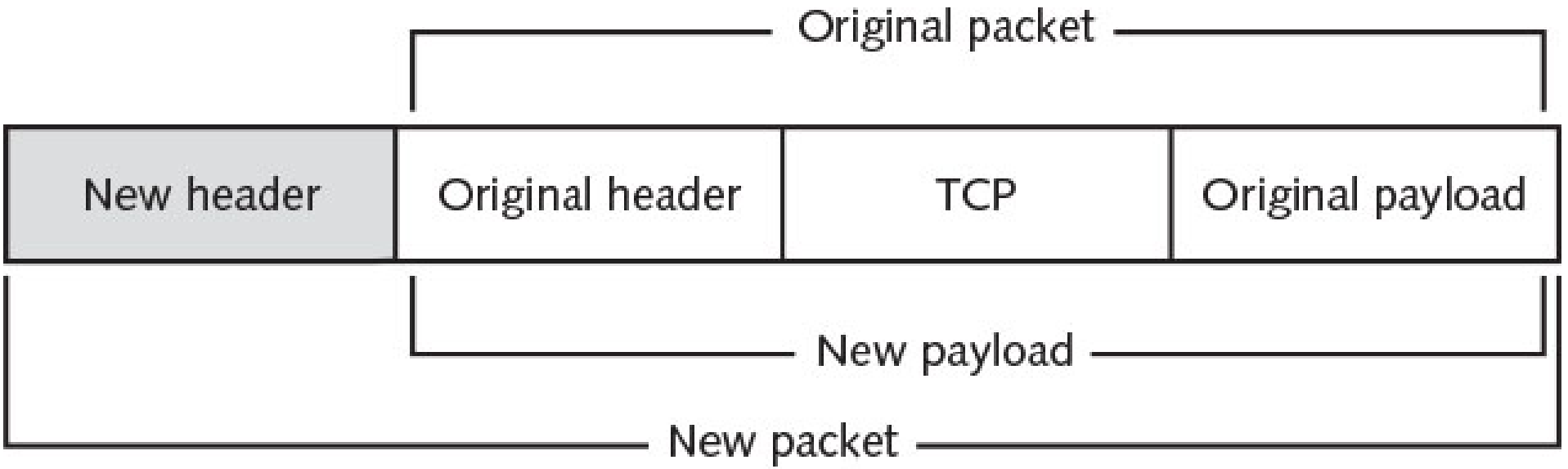

Figure 6-12 New IPsec packet using tunnel mode

Cryptographic Transport Protocols

IP Security (IPsec) —Cont.

- IPsec accomplishes transport and tunnel modes by adding new headers to the IP packet
- Entire original packet (header and payload) then treated as the data portion of the new packet
- Because tunnel mode protects the entire packet, it generally used in a network-to-network communication
- Transport mode is used when a device must see the source and destination addresses to route the packet

Quick Quiz

1. _____ is a framework for all of the entities involved in digital certificates (including hardware, software, people, policies and procedures) to create, store, distribute, and revoke digital certificates.
   Answer:

Quick Quiz

1. _____ is a framework for all of the entities involved in digital certificates (including hardware, software, people, policies and procedures) to create, store, distribute, and revoke digital certificates.
   Answer: Public key infrastructure (PKI)

Quick Quiz

1. _____ is a framework for all of the entities involved in digital certificates (including hardware, software, people, policies and procedures) to create, store, distribute, and revoke digital certificates.
   Answer: Public key infrastructure (PKI)

2. A(n) _____ refers to the type of trusting relationship that can exist between individuals or entities.
   Answer:

Quick Quiz

1. _____ is a framework for all of the entities involved in digital certificates (including hardware, software, people, policies and procedures) to create, store, distribute, and revoke digital certificates.
   Answer: Public key infrastructure (PKI)

2. A(n) _____ refers to the type of trusting relationship that can exist between individuals or entities.
   Answer: trust model

Quick Quiz

1. _____ is a framework for all of the entities involved in digital certificates (including hardware, software, people, policies and procedures) to create, store, distribute, and revoke digital certificates.
   Answer: Public key infrastructure (PKI)

2. A(n) _____ refers to the type of trusting relationship that can exist between individuals or entities.
   Answer: trust model

3. A(n) _____ is a published set of rules that govern the operation of a PKI.
   Answer:

Quick Quiz

1. _____ is a framework for all of the entities involved in digital certificates (including hardware, software, people, policies and procedures) to create, store, distribute, and revoke digital certificates.
   Answer: Public key infrastructure (PKI)

2. A(n) _____ refers to the type of trusting relationship that can exist between individuals or entities.
   Answer: trust model

3. A(n) _____ is a published set of rules that govern the operation of a PKI.
   Answer: certificate policy (CP)

Quick Quiz

1. _____ is a framework for all of the entities involved in digital certificates (including hardware, software, people, policies and procedures) to create, store, distribute, and revoke digital certificates.
   Answer: Public key infrastructure (PKI)

2. A(n) _____ refers to the type of trusting relationship that can exist between individuals or entities.
   Answer: trust model

3. A(n) _____ is a published set of rules that govern the operation of a PKI.
   Answer: certificate policy (CP)

4. A process in which keys are managed by a third party, such as a trusted CA, is known as _____.
   Answer:

Quick Quiz

1. _____ is a framework for all of the entities involved in digital certificates (including hardware, software, people, policies and procedures) to create, store, distribute, and revoke digital certificates.
   Answer: Public key infrastructure (PKI)

2. A(n) _____ refers to the type of trusting relationship that can exist between individuals or entities.
   Answer: trust model

3. A(n) _____ is a published set of rules that govern the operation of a PKI.
   Answer: certificate policy (CP)

4. A process in which keys are managed by a third party, such as a trusted CA, is known as _____.
   Answer: key escrow