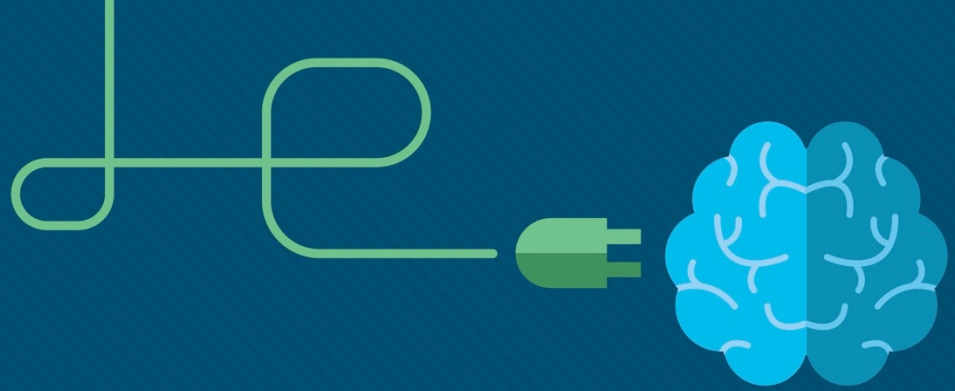


Chapter 7: Cryptography and the Public Key Infrastructure

Information Security

Dr. Ayman Aljarbouh

7.2 Public Key Cryptography

Module Objectives

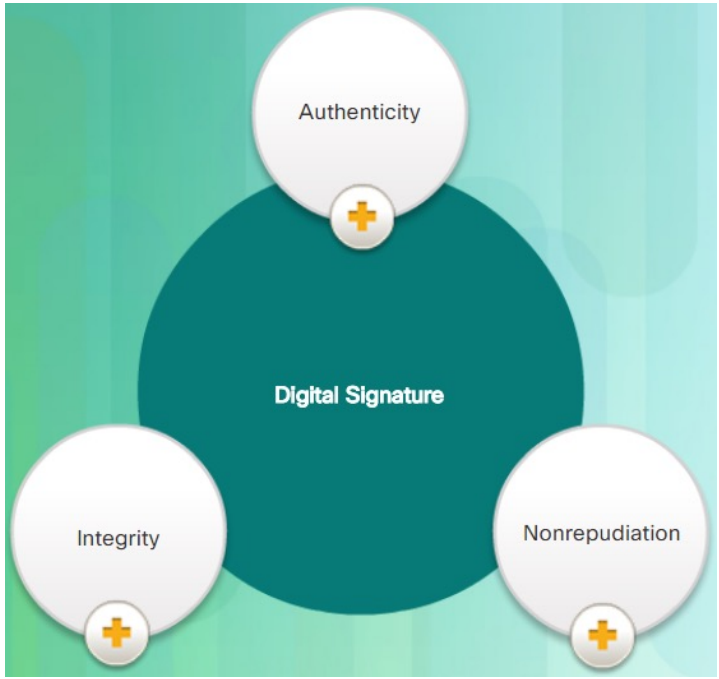
Module Title: Public Key Cryptography

Module Objective: Explain how the public key infrastructure (PKI) supports network security.

Topic Title	Topic Objective
Public Key Cryptography	Explain public key cryptography.
Authorities and the PKI Trust System	Explain how the public key infrastructure functions.
Applications and Impacts of Cryptography	Explain how the use of cryptography affects cybersecurity operations.

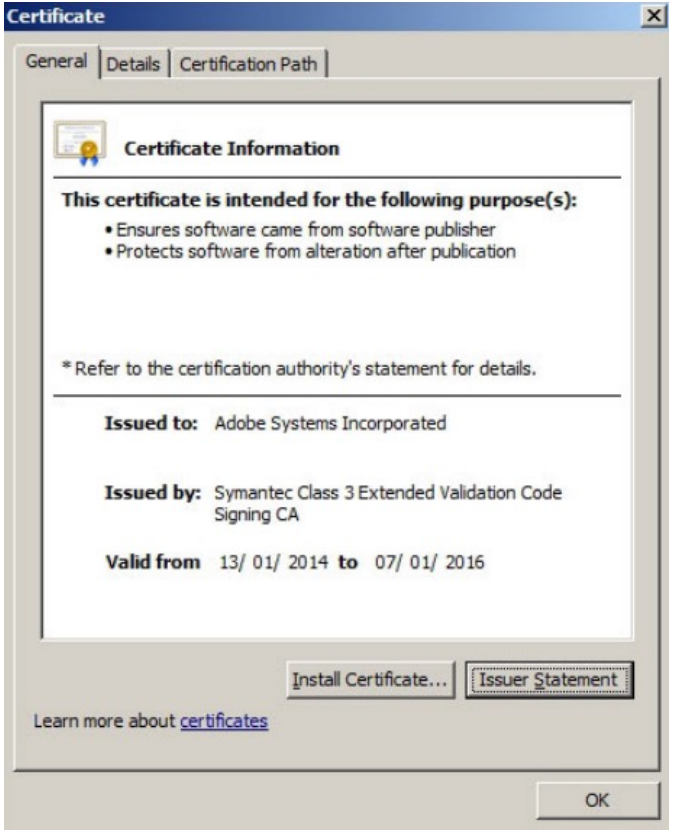
Using Digital Signatures

- Digital signatures are a mathematical technique used to provide authenticity, integrity, and nonrepudiation in the form of code signing and digital certificates.
- Digital signatures are commonly used in the following two situations:
  - **Code signing** –Code signing is used to verify the integrity of executable files downloaded from a vendor website.
  - **Digital certificates** – These are used to authenticate the identity of a system and exchange confidential data.
- There are three Digital Signature Standard (DSS) algorithms used for generating and verifying digital signatures:
  - **Digital Signature Algorithm (DSA)**
  - **Rivest-Shamir Adelman Algorithm (RSA)**
  - **Elliptic Curve Digital Signature Algorithm (ECDSA)**



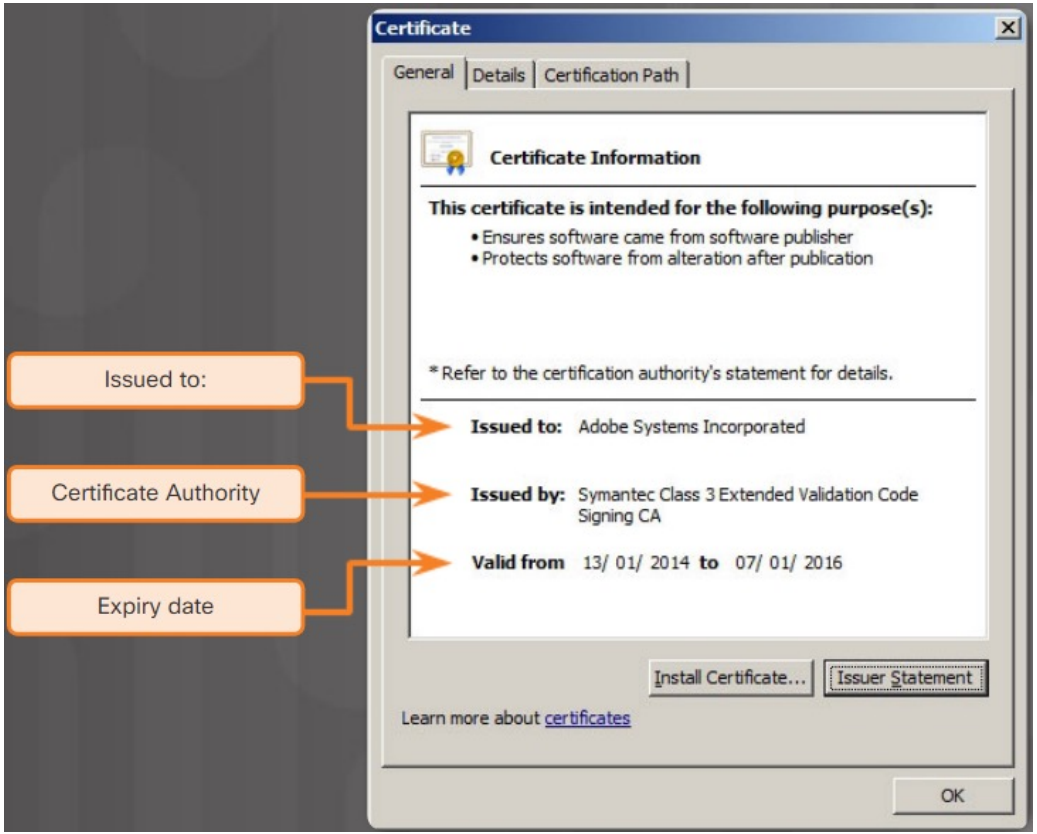
Digital Signatures for Code Signing

- Digital signatures are commonly used to provide assurance of the authenticity and integrity of software code.
- Executable files are wrapped in a digitally signed envelope, which allows the end user to verify the signature before installing the software.
- Digitally signing code provides several assurances about the code:
  - The code is authentic and is actually sourced by the publisher.
  - The code has not been modified since it left the software publisher.
  - The publisher undeniably published the code. This provides nonrepudiation of the act of publishing.



Digital Signatures for Digital Certificates

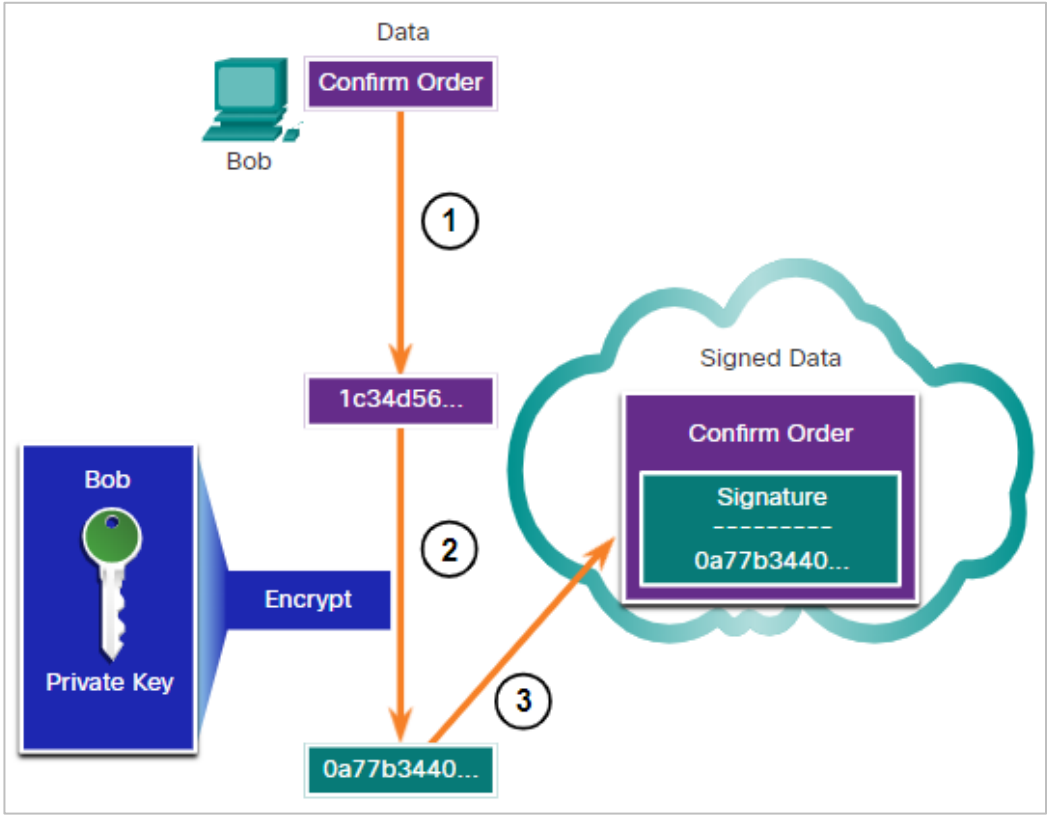
- A digital certificate enables users, hosts, and organizations to securely exchange information over the Internet.
- Specifically, a digital certificate is used to authenticate and verify that users sending a message are who they claim to be.
- Digital certificates can also be used to provide confidentiality for the receiver with the means to encrypt a reply.



Digital Signatures for Digital Certificates (Contd.)

This scenario will help you understand how a digital signature is used.

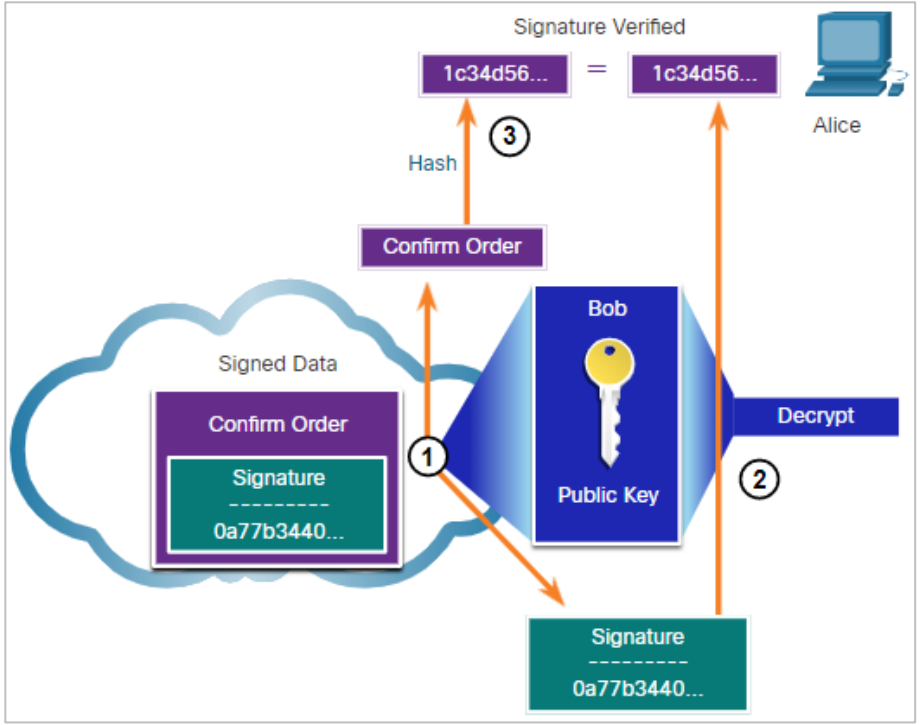
- Bob is confirming an order with Alice, which she is ordering from Bob's website.
- Bob confirms the order and his computer creates a hash of the confirmation.
- The computer encrypts the hash with Bob's private key.
- The encrypted hash, which is the digital signature, is added to the document.
- The order confirmation is then sent to Alice over the internet.



Digital Signatures for Digital Certificates (Contd.)

When Alice receives the digital signature, the following process occurs:

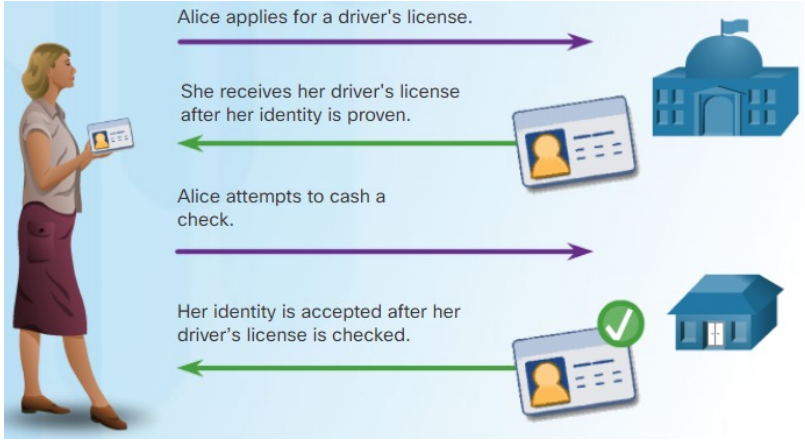
- Alice's receiver accepts the order confirmation with the digital signature and obtains Bob's public key.
- Alice's computer then decrypts the signature using Bob's public key which reveals the assumed hash value of the sending device.
- Alice's computer creates a hash of the received document, without its signature, and compares this hash to the decrypted hash.
- If the hashes match, the document is authentic. This means the confirmation was sent by Bob and has not changed since signed.



Public Key Management

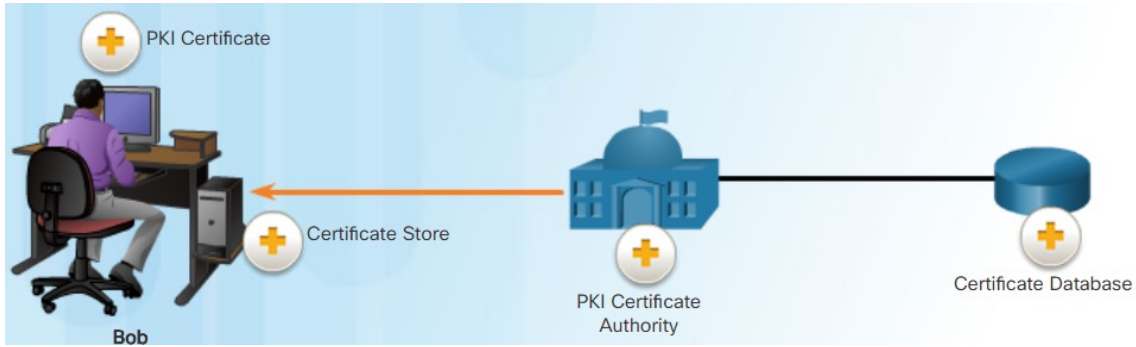
- When establishing an asymmetric connection between two hosts, the hosts will exchange their public key information.
- Trusted third parties on the Internet validate the authenticity of these public keys using digital certificates. The third party issues credentials that are difficult to forge.
- From that point forward, all individuals who trust the third party simply accept the credentials that the third party issues.

- The Public Key Infrastructure (PKI) is an example of a trusted third-party system referred to as certificate authority (CA).
- The CA issues digital certificates that authenticate the identity of organizations and users.
- These certificates are also used to sign messages to ensure that the messages have not been tampered with.



The Public Key Infrastructure

- PKI is needed to support large-scale distribution and identification of public encryption keys.
- The PKI framework facilitates a highly scalable trust relationship.
- It consists of the hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates.
- Not all PKI certificates are directly received from a CA. A registration authority (RA) is a subordinate CA and is certified by a root CA to issue certificates for specific uses.



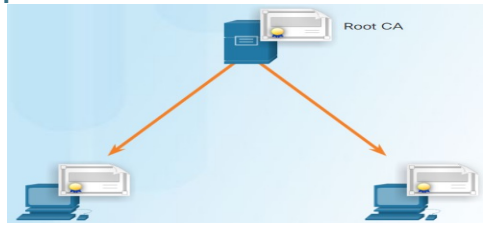
The PKI Authorities System

- Many vendors provide CA servers as a managed service or as an end-user product.
- Organizations may also implement private PKIs using Microsoft Server or Open SSL.
- CAs issue certificates based on classes which determine how trusted a certificate is.
- The class number is determined by how rigorous the procedure was that verified the identity of the holder when the certificate was issued.
- The higher the class number, the more trusted the certificate.
- Some CA public keys are preloaded, such as those listed in web browsers.
- An enterprise can also implement PKI for internal use.

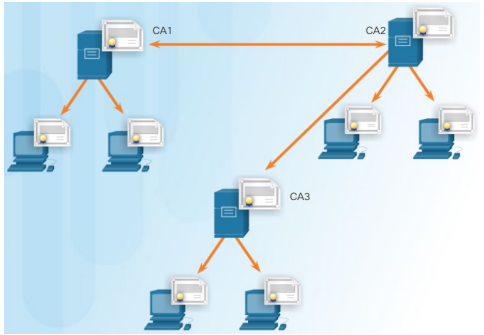
Class	Description
0	Used for testing purposes in which no checks have been performed.
1	Used for individuals with a focus on verification of email.
2	Used for organizations for which proof of identity is required.
3	Used for servers and software signing for which independent verification and checking of identity and authority is done by the issuing certificate authority.
4	Used for online business transactions between companies.
5	Used for private organizations or governmental security.

The PKI Trust System

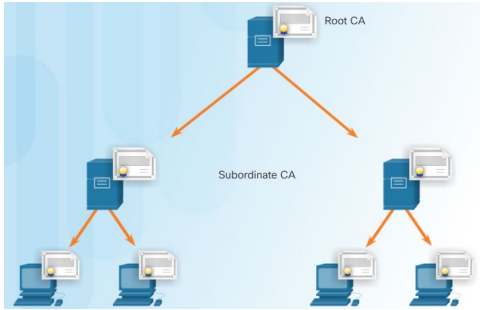
- PKIs can form different topologies of trust. The simplest is the single-root PKI topology. On larger networks, PKI CAs may be linked using two basic architectures:
  - **Cross-certified CA topologies** - This a peer-to-peer model in which individual CAs establish trust relationships with other CAs by cross-certifying CA certificates.
  - **Hierarchical CA topologies** - The highest level CA is called the root CA. It can issue certificates to end users and to a subordinate CA.



Single-Root PKI



Cross-certified CA



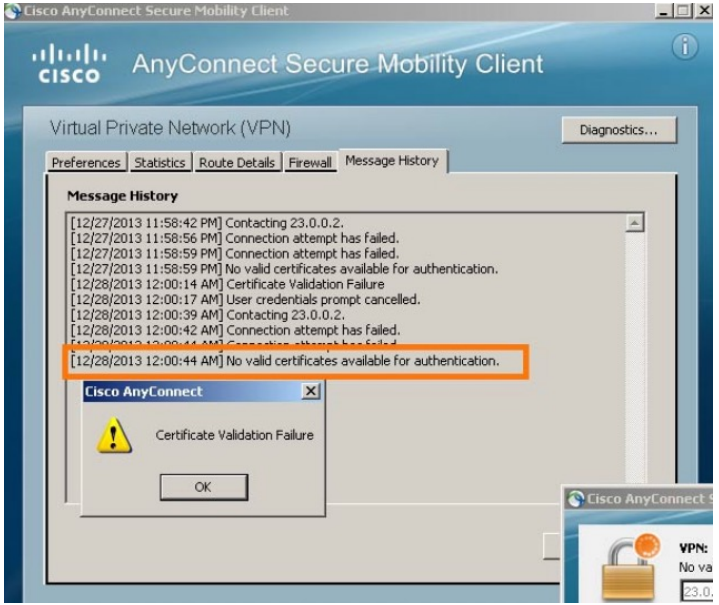
Hierarchical CA

PKI Applications

- Some of the many applications of PKIs are:
  - SSL/TLS certificate-based peer authentication
  - Secure network traffic using IPsec VPNs
  - HTTPS Web traffic
  - Control access to the network using 802.1x authentication
  - Secure email using the S/MIME protocol
  - Secure instant messaging
  - Approve and authorize applications with Code Signing
  - Protect user data with the Encryption File System (EFS)
  - Implement two-factor authentication with smart cards
  - Securing USB storage devices

Encrypted Network Transactions

- Threat actors can use SSL/TLS to introduce regulatory compliance violations, viruses, malware, data loss, and intrusion attempts in a network.
- Other SSL/TLS-related issues may be associated with validating the certificate of a web server. When this occurs, web browsers will display a security warning. PKI-related issues that are associated with security warnings include:
  - **Validity date range** - The X.509v3 certificates specify “not before” and “not after” dates. If the current date is outside the range, the web browser displays a message.
  - **Signature validation error** - If a browser cannot validate the signature on the certificate, there is no assurance that the public key in the certificate is authentic.



Encryption and Security Monitoring

- Network monitoring becomes more challenging when packets are encrypted.
- Because HTTPS introduces end-to-end encrypted HTTP traffic (via TLS/SSL), it is not as easy to peek into user traffic.
- Here is a list of some of the things that a security analyst could do:
  - Configure rules to distinguish between SSL and non-SSL traffic, HTTPS and non-HTTPS SSL traffic.
  - Enhance security through server certificate validation using CRLs and OCSP.
  - Implement antimalware protection and URL filtering of HTTPS content.
  - Deploy a Cisco SSL Appliance to decrypt SSL traffic and send it to intrusion prevention system (IPS) appliances to identify risks normally hidden by SSL.

New Terms and Commands

• Certificate Authority (CA) • Certificate Revocation List (CRL) • Online Certificate Status Protocol (OCSP) • Elliptic Curve Digital Signature Algorithm (ECDSA)	• Public Key Infrastructure (PKI) • Secure Socket Layer (SSL) • Digital Signature Algorithm (DSA) • Digital Signature Standard (DSS)

Lab 29 – Certificate Authority Stores

In this lab, you will complete the following objectives:

- Certificates Trusted by Your Browser
- Checking for Man-In-Middle