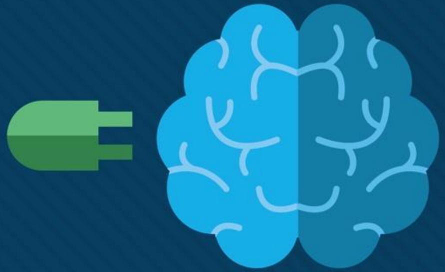
Key Management.
Cryptography applications.



Cryptanalysis – Code Breaking

- A number of code breaking (cryptanalysis) methods exist, such as brute-force, ciphertext, and known-plaintext, among others.

- Several methods are used in cryptanalysis:
  - **Brute-force** - The cryptanalyst tries every possible key knowing that eventually one of them will work.
  - **Ciphertext** - The cryptanalyst has the ciphertext of several encrypted messages but no knowledge of the underlying plaintext.
  - **Known-Plaintext** - The cryptanalyst has access to the ciphertext of several messages and knows something about the plaintext underlying that ciphertext.
  - **Chosen-Plaintext** - The cryptanalyst chooses which data the encryption device encrypts and observes the ciphertext output.
  - **Chosen-Ciphertext** - The cryptanalyst can choose different ciphertext to be decrypted and has access to the decrypted plaintext.
  - **Meet-in-the-Middle** - The cryptanalyst knows a portion of the plaintext and the corresponding ciphertext.

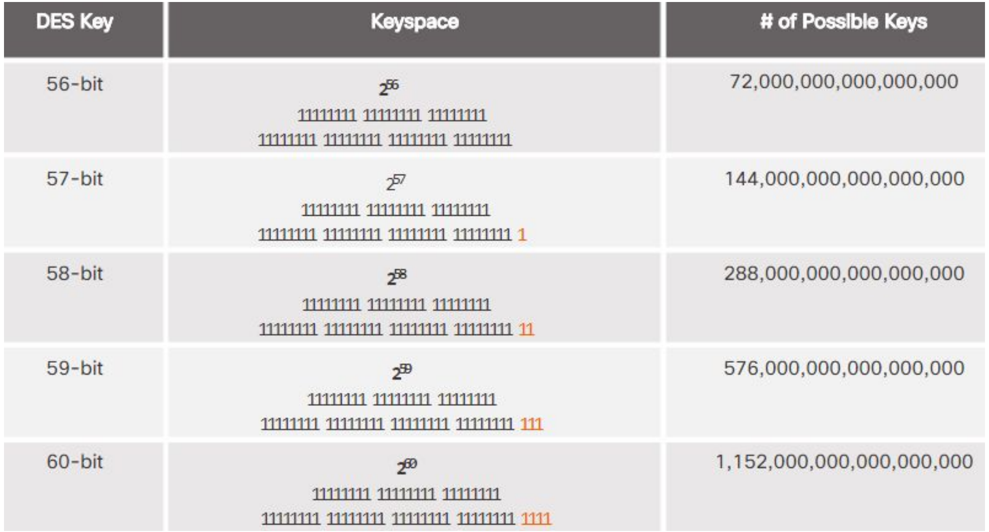
Keys

- With modern technology, security of encryption lies in the secrecy of the keys, not the algorithm.

Two terms that are used to describe keys are:

- **Key length** - Also called the key size, this is measured in bits. In this course, we will use the term key length.
- **Keyspace** - This is the number of possibilities that can be generated by a specific key length.

- As key length increases, the keyspace increases exponentially.

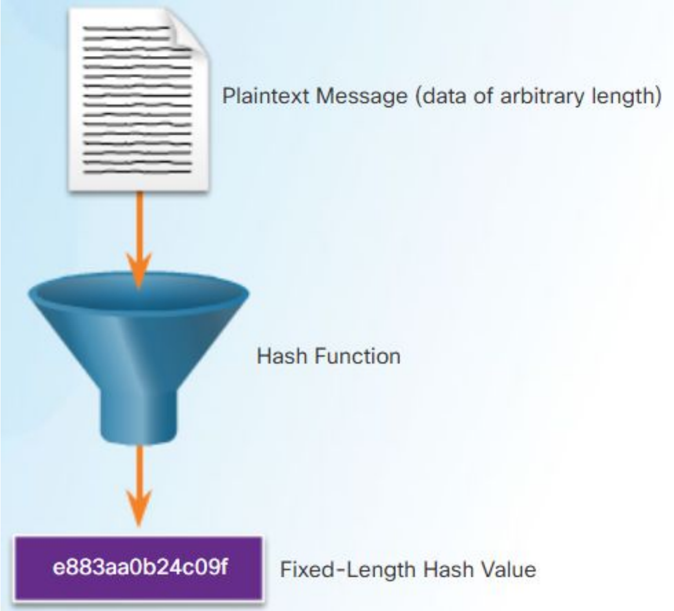


DES Key	Keyspace	# of Possible Keys
56-bit	2^{56} 11111111 11111111 11111111 11111111 11111111 11111111 11111111	72,000,000,000,000,000
57-bit	2^{57} 11111111 11111111 11111111 11111111 11111111 11111111 11111111 1	144,000,000,000,000,000
58-bit	2^{58} 11111111 11111111 11111111 11111111 11111111 11111111 11111111 11	288,000,000,000,000,000
59-bit	2^{59} 11111111 11111111 11111111 11111111 11111111 11111111 11111111 111	576,000,000,000,000,000
60-bit	2^{60} 11111111 11111111 11111111 11111111 11111111 11111111 11111111 1111	1,152,000,000,000,000,000

Integrity and Authenticity

Cryptographic Hash Functions

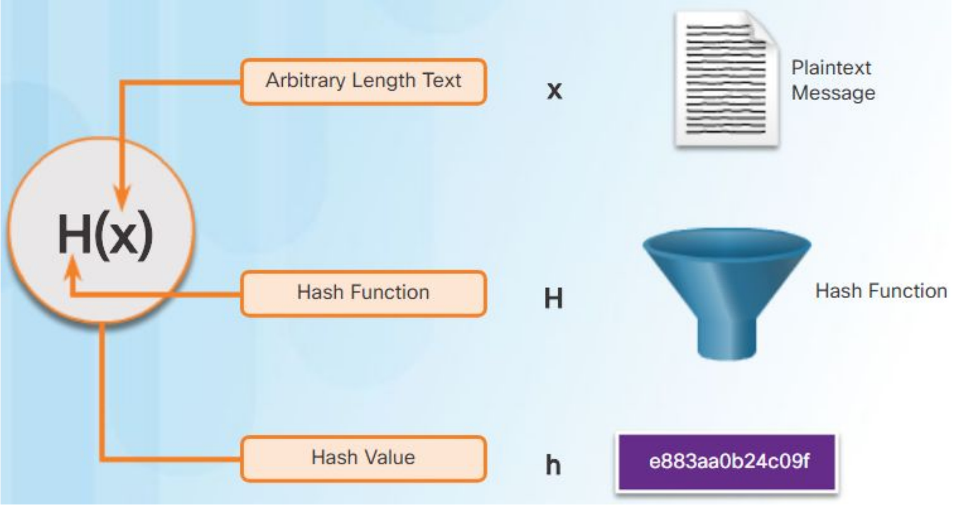
- Cryptographic hashes are used to verify and ensure data integrity.
- Hashing is based on a one-way mathematical function that is relatively easy to compute, but significantly harder to reverse.
- The cryptographic hashing function can also be used to verify authentication.
- A hash function takes a variable block of binary data, called the message, and produces a fixed-length, condensed representation, called the hash.
- The resulting hash is also sometimes called the message digest, digest, or digital fingerprint.
- With hash functions, it is computationally infeasible for two different sets of data to come up with the same hash output.
- Every time the data is changed or altered, the hash value also changes.



Integrity and Authenticity

Cryptographic Hash Operation

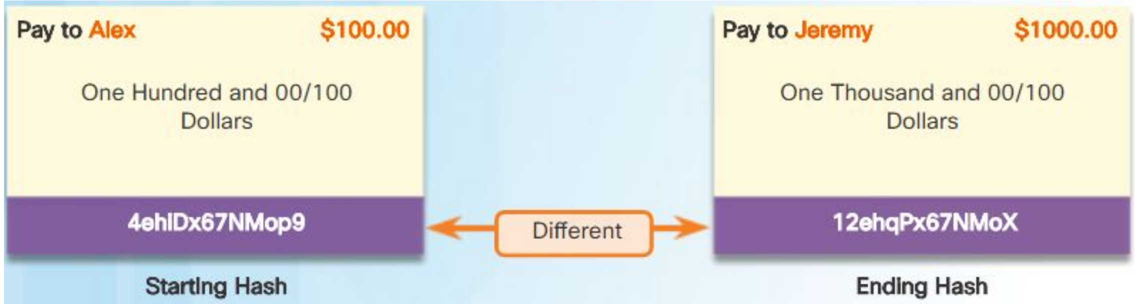
- Mathematically, the equation ***h= H(x)*** is used to explain how a hash algorithm operates.
- A cryptographic hash function should have the following properties:
  - The input can be any length.
  - The output has a fixed length.
  - H(x) is relatively easy to compute for any given x.
  - H(x) is one way and not reversible.
  - H(x) is collision free, meaning that two different input values will result in different hash values.



Integrity and Authenticity

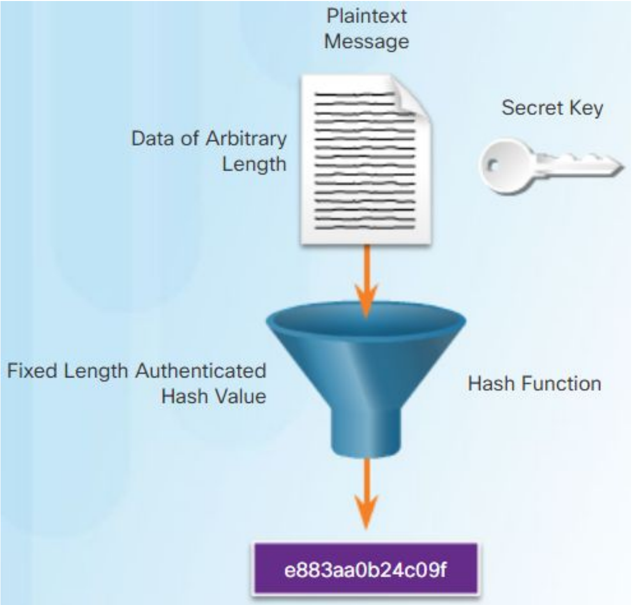
MD5 and SHA

- Hash functions are used to ensure the integrity of a message. They ensure data has not changed accidentally or intentionally.
- Three well-known hashing algorithms are 128-bit MD5, SHA-1, and SHA-2.
  - **MD5 with 128-bit digest** - A one-way function that produces a 128-bit hashed message. MD5 is considered to be a legacy algorithm. It is recommended that SHA-2 be used instead.
  - **SHA-1** – Very similar to the MD5 hash functions. Several versions exist. SHA-1 creates a 160 bit hashed message and is slightly slower than MD5. SHA-1 has known flaws and is a legacy algorithm.
  - **SHA-2** –Next-generation algorithm and should be used whenever possible.
- While hashing can be used to detect accidental changes, it cannot be used to guard against deliberate changes. There is no unique identifying information from the sender in the hashing procedure.



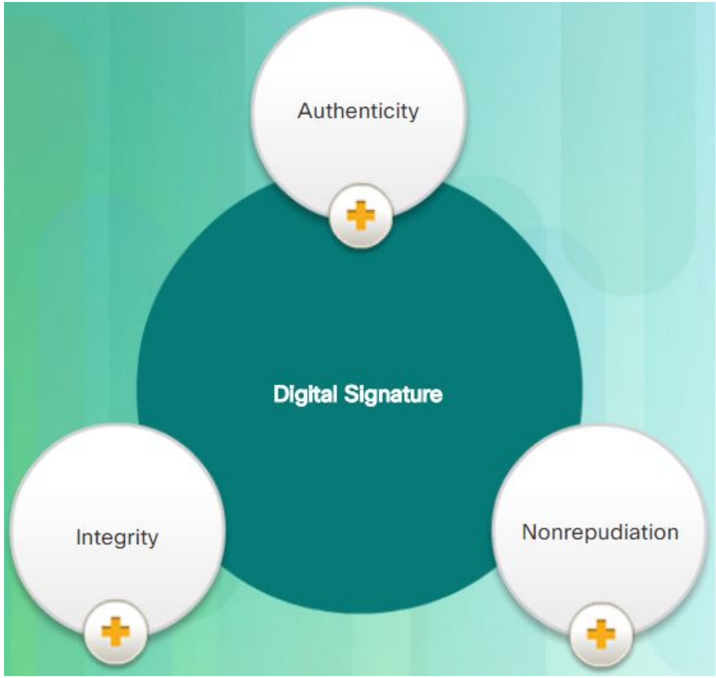
Hash Message Authentication Code

- To add authentication to integrity assurance, a keyed-hash message authentication code (HMAC) is used.
- To add authentication, HMAC uses an additional secret key as input to the hash function.
- Only the sender and the receiver know the secret key, and the output of the hash function now depends on the input data and the secret key.
- Only parties who have access to that secret key can compute the digest of an HMAC function.
- If the digest that is calculated by the receiving device is equal to the digest that was sent, the message has not been altered.



Public Key Cryptography
Using Digital Signatures

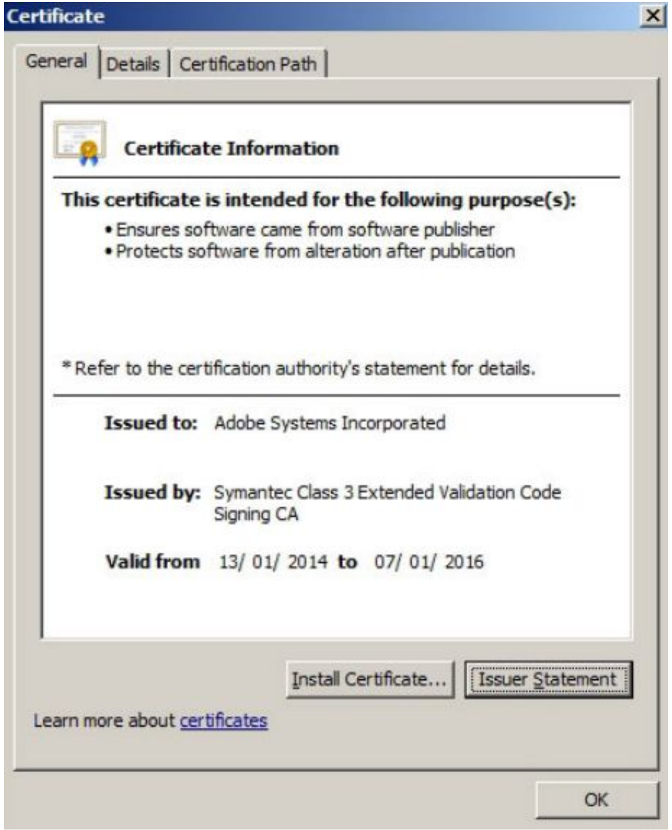
- Digital signatures are a mathematical technique used to provide authenticity, integrity, and nonrepudiation in the form of code signing and digital certificates.
- Digital signatures are commonly used in the following two situations:
  - **Code signing** –Code signing is used to verify the integrity 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)**



Public Key Cryptography

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.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

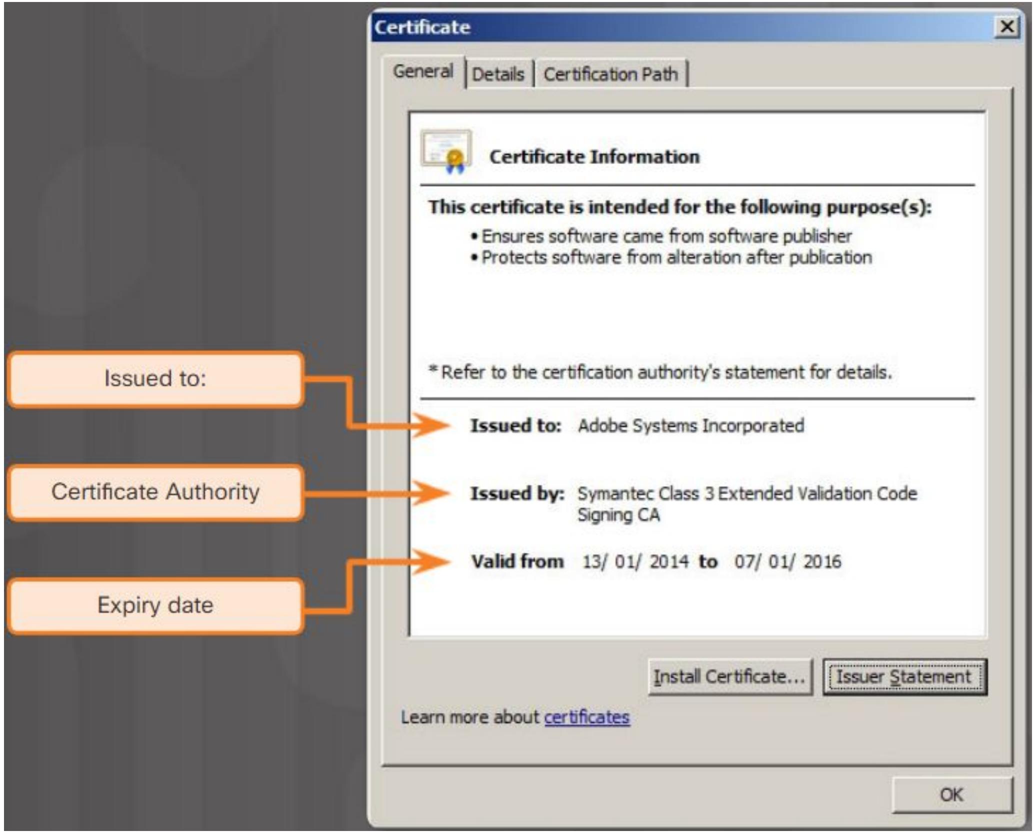
Issued to: Adobe Systems Incorporated

Issued by: Symantec Class 3 Extended Validation Code Signing CA

Valid from 13/ 01/ 2014 **to** 07/ 01/ 2016

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.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: Adobe Systems Incorporated

Issued by: Symantec Class 3 Extended Validation Code Signing CA

Valid from 13/ 01/ 2014 **to** 07/ 01/ 2016

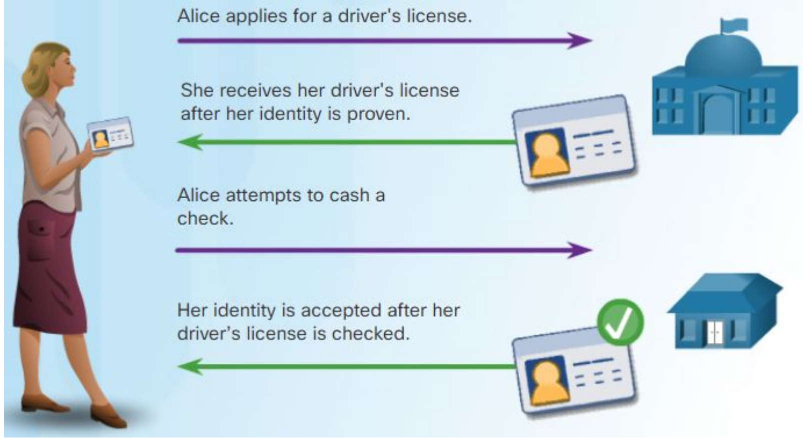
Learn more about certificates

Authorities and the PKI Trust System

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.



Alice applies for a driver's license.

She receives her driver's license after her identity is proven.

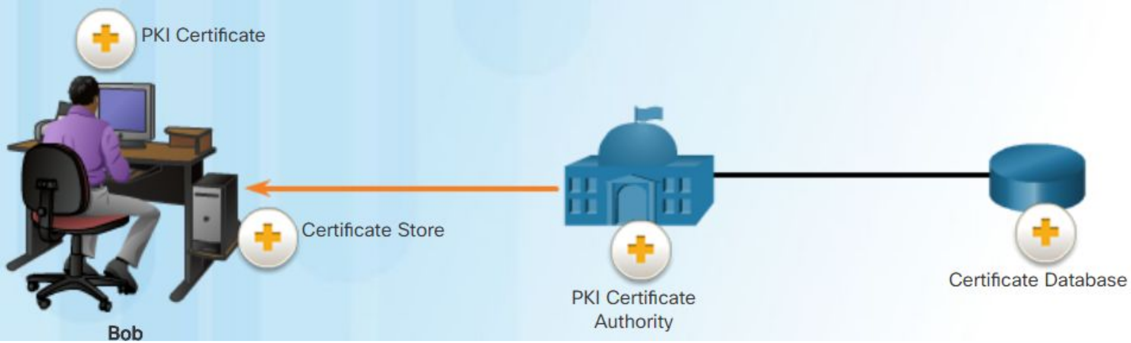
Alice attempts to cash a check.

Her identity is accepted after her driver's license is checked.

Authorities and the PKI Trust System

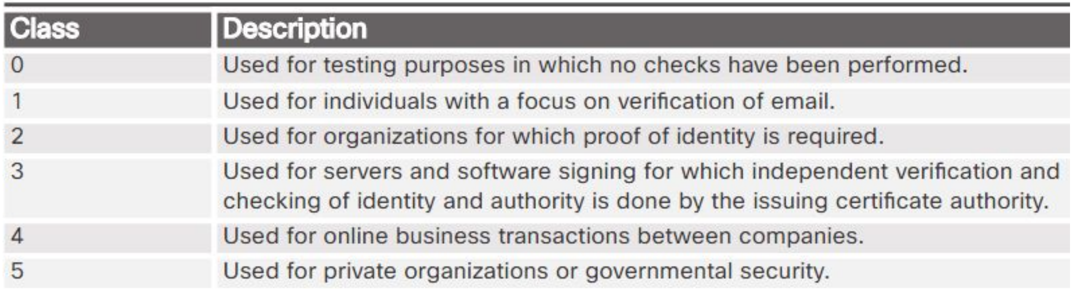
The Public Key Infrastructure

- 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.

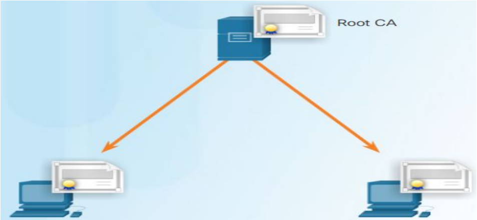
Authorities and the PKI Trust System

The PKI Trust System

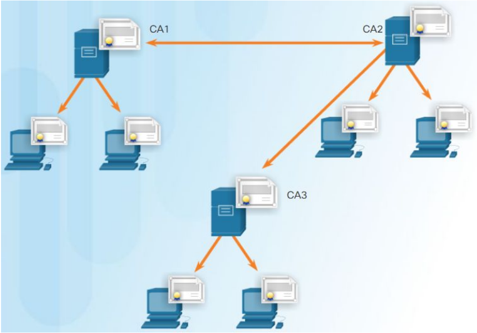
- PKIs can form different topologies of trust. The simplest is the single-root PKI topology.

On larger networks, PKI CAs may be linked using two basic architectures:

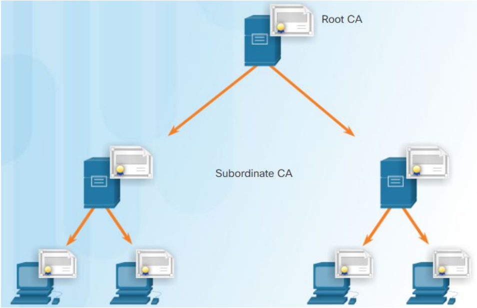
- **Cross-certified CA topologies** - This a peer-to-peer model in which individual CAs establish trust relationships with other CAs by cross-certifying CA certificates.
- **Hierarchical CA topologies** - The highest level CA is called the root CA. It can issue certificates to end users and to a subordinate CA.



Single-Root PKI



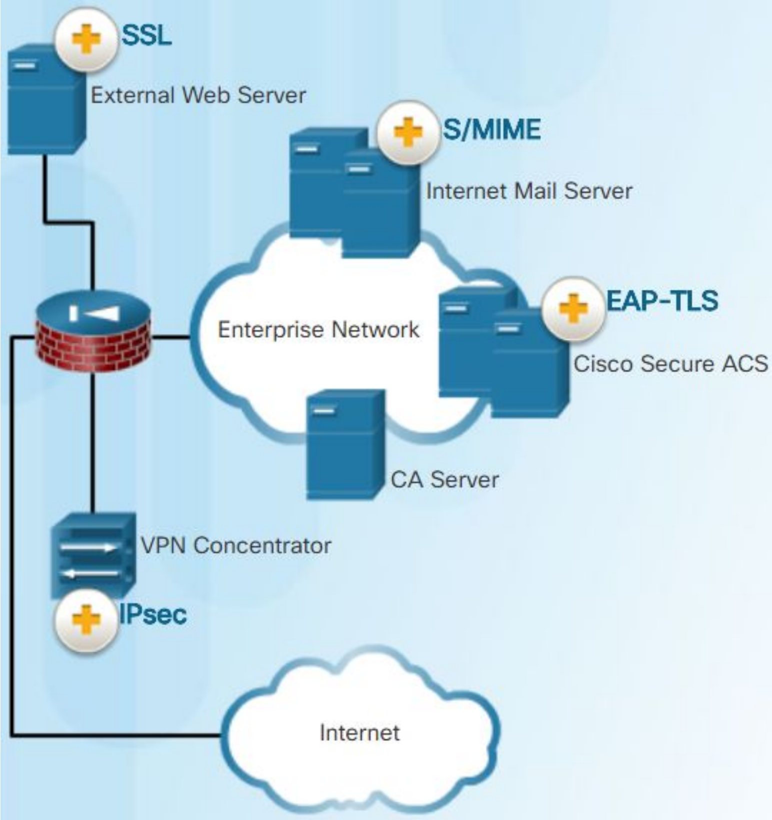
Cross-certified CA



Hierarchical CA

Interoperability of Different PKI Vendors

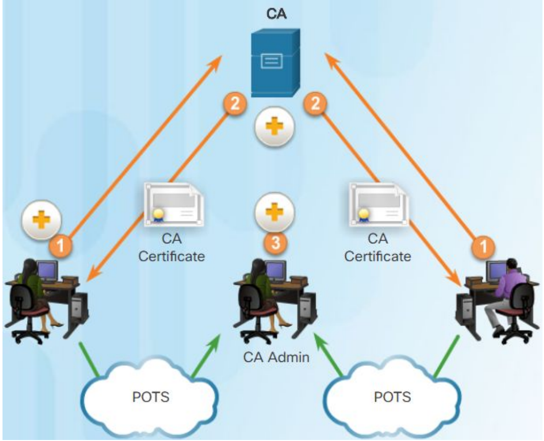
- Interoperability between a PKI and its supporting services is a concern because many CA vendors have proposed and implemented proprietary solutions instead of waiting for standards to develop.
- To address this interoperability concern, the IETF published the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527).
- The X.509 version 3 (X.509v3) standard defines the format of a digital certificate.



Authorities and the PKI Trust System

Certificate Enrollment, Authentication, and Revocation

- All systems that leverage the PKI must have the CA's public key, called the self-signed certificate.
- The CA public key verifies all the certificates issued by the CA and is vital for the proper operation of the PKI.
- The certificate enrollment process begins when CA certificates are retrieved in-band over a network, and the authentication is done out-of-band (OOB) using the telephone.
- The system enrolling with the PKI contacts a CA to request and obtain a digital identity certificate for itself and to get the CA's self-signed certificate.
- The final stage verifies that the CA certificate was authentic and is performed using an OOB method such as the Plain Old Telephone System (POTS) to obtain the fingerprint of the valid CA identity certificate.
- A digital certificate can be revoked if key is compromised or if it is no longer needed.



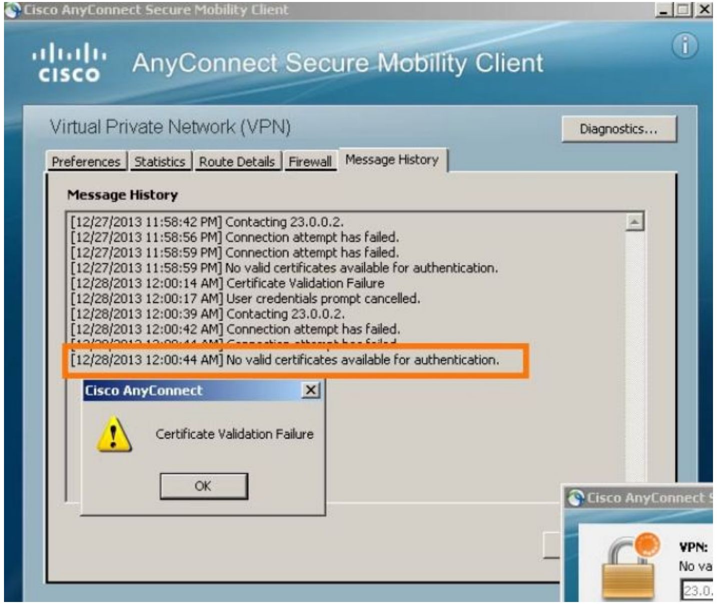
Applications and Impacts of Cryptography

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

Encrypting 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.


Cisco AnyConnect Secure Mobility Client
cisco
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Diagnostics...
Preferences
Statistics
Route Details
Firewall
Message History

Message History

```
[12/27/2013 11:58:42 PM] Contacting 23.0.0.2.
[12/27/2013 11:58:56 PM] Connection attempt has failed.
[12/27/2013 11:58:59 PM] Connection attempt has failed.
[12/27/2013 11:58:59 PM] No valid certificates available for authentication.
[12/28/2013 12:00:14 AM] Certificate Validation Failure
[12/28/2013 12:00:17 AM] User credentials prompt cancelled.
[12/28/2013 12:00:39 AM] Contacting 23.0.0.2.
[12/28/2013 12:00:42 AM] Connection attempt has failed.
[12/28/2013 12:00:44 AM] No valid certificates available for authentication.
```

Cisco AnyConnect

Certificate Validation Failure

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.