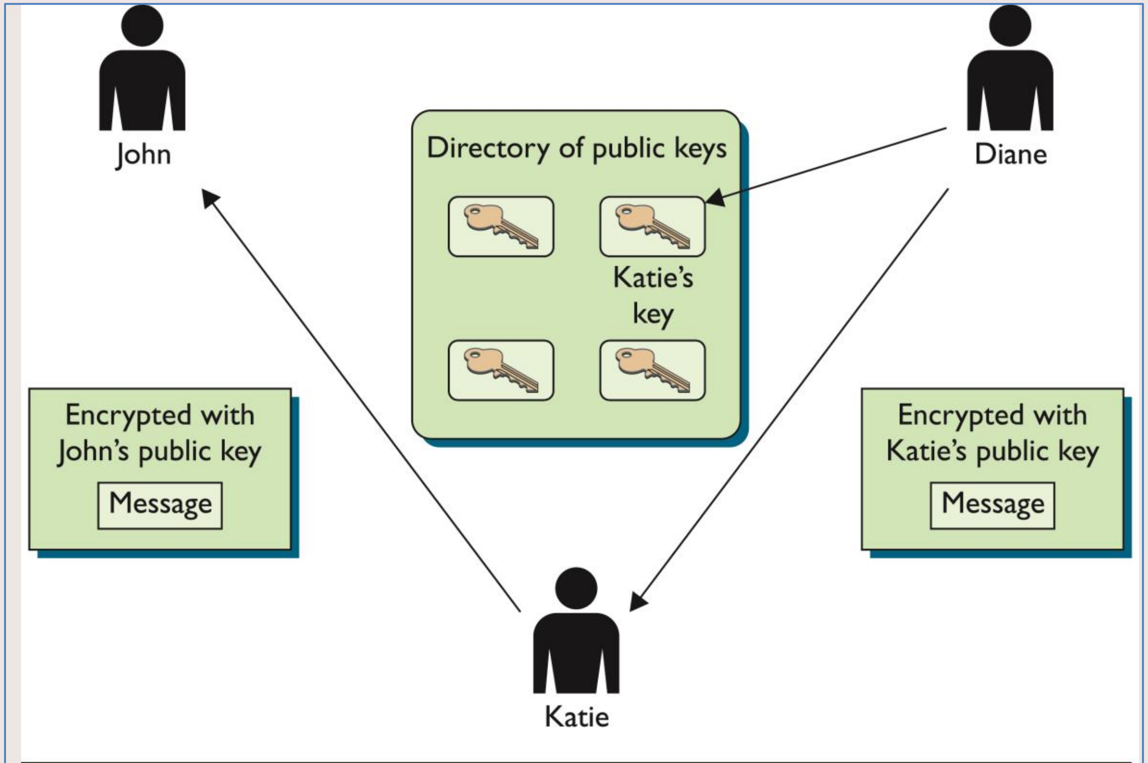
Public Key Infrastructure (PKI)

Can You Trust That Key?


John
Directory of public keys
Katie's key
Diane
Encrypted with John's public key
Message
Encrypted with Katie's public key
Message
Katie

Man-in-the-Middle Attack

1. Katie replaces John's public key with her key in the publicly accessible directory.
2. Diane extracts what she thinks is John's key, but it is in fact Katie's key.
3. Katie can now read messages Diane encrypts and sends to John.
4. After Katie decrypts and reads Diane's message, she encrypts it with John's public key and sends it on to him so he will not be the wiser.

Public Key Infrastructure (PKI)

- ❑ Manages the sharing of trust using a third party to vouch for the trustworthiness of a claim of ownership over a credential document, called a *certificate.*
- ❑ Facilitates the use of public key cryptography for digital signatures and integrity while facilitates symmetric cryptography for data encryption.
- ❑ Allows for different types of users and entities to be able to communicate securely and in a predictable manner.
- ❑ PKI is made up of hardware, applications, policies, services, programming interfaces, cryptographic algorithms, protocols, users, and utilities.
- ❑ PKI is a framework (Guideline) not a specific technology.
- ❑ Universal Infrastructure that can work across multiple systems and vendors.

Public Key Infrastructure (PKI)

A PKI provide the following:

Authentication: This can be defined as a means of identification. PKI offers this ***through digital certificates.***

Non repudiation: The basis of non-repudiation is that the sender cannot disown any information sent at a later time. Non-repudiation ensures that there is trustworthy means of ensuring ownership of an electronic document. PKI offers non-repudiation **through digital signatures.**

Confidentiality: This can be defined as the secure transmission of information over networks ensuring that it is not accessed by unauthorized individuals. PKI ensures confidentiality **through use of encryption algorithms.**

Integrity: The concept of data integrity is that data should not be altered of modified in any way while traversing the network. Integrity of data is ensured **by message hashing.**

Access Control: The idea of access control is to ensure that only people with the required security privileges are allowed access to information. PKI ensures access control **through public and private key pairs.**

Basics of Public Key Infrastructures

- ❑ PKI environments use entities called registration authorities (RAs) and certificate authorities (CAs).
- ❑ PKIs work like the DMV(Drive license Dept.).
  - ❖ You prove you who you are to the DMV by bringing the information they require.
  - ❖ If you have met the requirements, you are issued an Identification card.
  - ❖ When people ask you who you are, you show the ID from the DMV.
  - ❖ They should now believe you are who you say you are.

DMV … Department of Motor Vehicles

Registration Authorities (RA)

- ❑ RA verifies user requests for a digital certificate and tells the Certificate Authority (CA) to issue it.
- ❑ An RA is a PKI component that accepts a request for a digital certificate and performs the steps of registering and authenticating the person requesting the certificate.
- ❑ The authentication requirements differ depending on the type of certificate being requested.
- ❑ Most CAs offer a series of classes of certificates with increasing trust by class.

Local Registration Authorities (LRA)

- ❑ Performs the same functions as an RA.
- ❑ Implemented in companies that have their own internal PKIs and have distributed sites.
- ❑ Instead of requiring users to communicate with a central RA, each site can have its own LRA.
- ❑ Reduces the traffic created by several users making requests across wide area network (WAN) lines.

Certificate Authorities (CA)

- ❑ CAs are a trusted authority that certifies identities and creates digital certificates.
- ❑ Digital certificates establish an association between the subject's identity and a public key.
- ❑ The private key that is paired with the public key in the certificate and is stored separately.
- ❑ Certificate server is the service that issues certificates:
  - ❖ Constructs the digital certificate and combines the user's public key with the resulting certificate.
  - ❖ The certificate is digitally signed with the CA's private key.

Certificate Authorities (CA)

Key Functions of CA

- ❑ Generating key pairs – The CA may generate a key pair independently or jointly with the client.
- ❑ Issuing digital certificates – The CA could be thought of as the PKI equivalent of a passport agency – the CA issues a certificate after client provides the credentials to confirm his identity. The CA then signs the certificate to prevent modification of the details contained in the certificate.
- ❑ Publishing Certificates – The CA need to publish certificates so that users can find them. There are two ways of achieving this. One is to publish certificates in the equivalent of an electronic telephone directory. The other is to send your certificate out to those people you think might need it by one means or another.

Certificate Authorities (CA)

Key Functions of CA

- ❑ Verifying Certificates – The CA makes its public key available in environment to assist verification of his signature on clients' digital certificate.

- ❑ Revocation of Certificates – At times, CA revokes the certificate issued due to some reason such as compromise of private key by user or loss of trust in the client. After revocation, CA maintains the list of all revoked certificate (CRL) that is available to the environment.

Certificate Revocation List (CRL)

- A Certificate Revocation List (CRL) is a list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted.
- CRLs are a type of blacklist and are used by various endpoints, including Web browsers, to verify whether a certificate is valid and trustworthy.

Certificate Repositories

- ❑ A centralized directory of public keys and certificates that can be accessed by a subset of individuals.
- ❑ If a person wants to encrypt the first message to the receiver, the sender needs to find the receiver's public key in a certificate repository.

Certificate Classes

Class	Typical Use
1	This is used to verify an individual's identity through e-mail. A person who receives a Class 1 certificate can use his public/private key pair to digitally sign e-mail and encrypt message contents.
2	This is for software signing. A software vendor would register for this type of certificate so that it could digitally sign its software. This provides integrity for the software after it is developed and released, and it allows the receiver of the software to verify from where the software actually came.
3	This is for a company to set up its own CA, which will allow it to carry out its own identification verification and generate certificates internally.

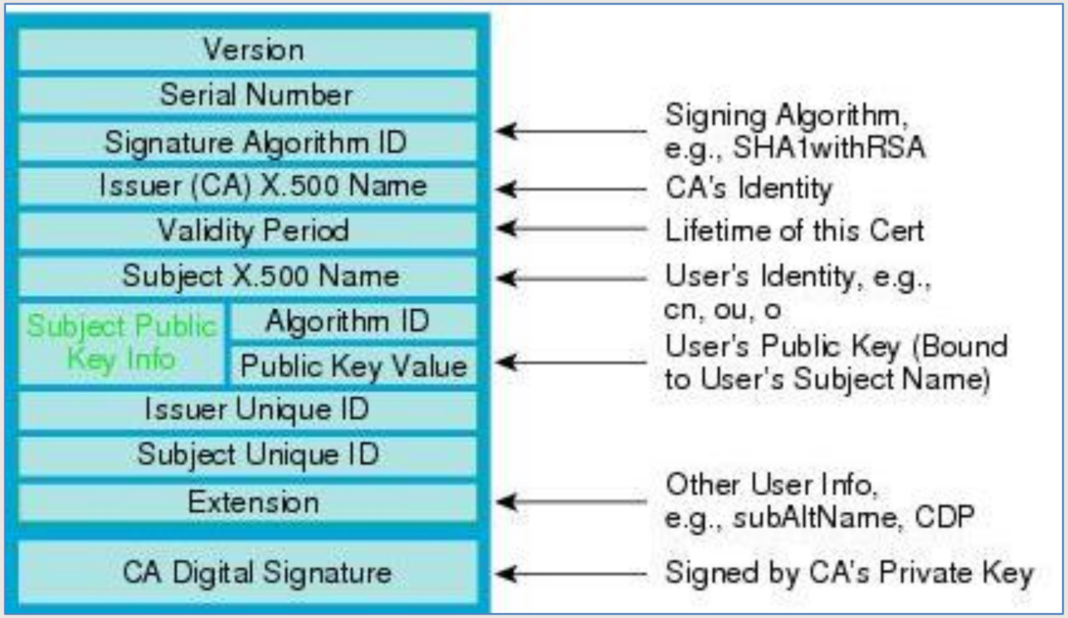
Digital Certificates

- ❑ A digital certificate binds an individual's identity to a public key.
  - ❖ Contains all information a receiver needs to be assured of the identity of the public key owner.
- ❑ The certificates are created and formatted based on the X.509 standard.
  - ❖ International Telecommunication Union (www.itu.int).
  - ❖ It outlines the necessary fields and values of a certificate.
  - ❖ As of this writing, version 3 is the most current

Certificate Details

A certificate is basically composed of two elements:

- ❑ User credentials:
  - ❖ such as the hostname, common name (CN), serial number, and public key—and other elements.



Version		
Serial Number		
Signature Algorithm ID		Signing Algorithm, e.g., SHA1withRSA
Issuer (CA) X.500 Name		CA's Identity
Validity Period		Lifetime of this Cert
Subject X.500 Name		User's Identity, e.g., cn, ou, o
Subject Public Key Info	Algorithm ID	
	Public Key Value	User's Public Key (Bound to User's Subject Name)
Issuer Unique ID		
Subject Unique ID		
Extension		Other User Info, e.g., subAltName, CDP
CA Digital Signature		Signed by CA's Private Key

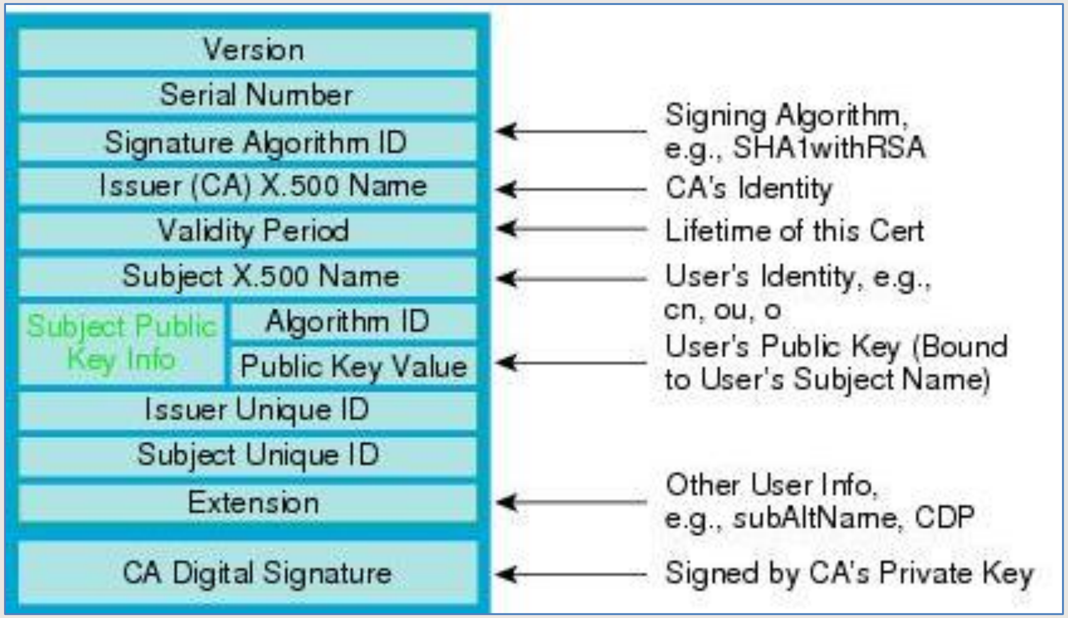
- ❖ The most important element of the certificate is the public key because all crypto-algorithms depend upon the public key.

Certificate Details

A certificate is basically composed of two elements:

- Digital signature of a CA server

- The digital signature for the trusted public authority that is trusted by both parties.



Version

Serial Number

Signature Algorithm ID ← Signing Algorithm, e.g., SHA1withRSA

Issuer (CA) X.500 Name ← CA's Identity

Validity Period ← Lifetime of this Cert

Subject X.500 Name ← User's Identity, e.g., cn, ou, o

Subject Public Key Info: Algorithm ID

Subject Public Key Info: Public Key Value ← User's Public Key (Bound to User's Subject Name)

Issuer Unique ID

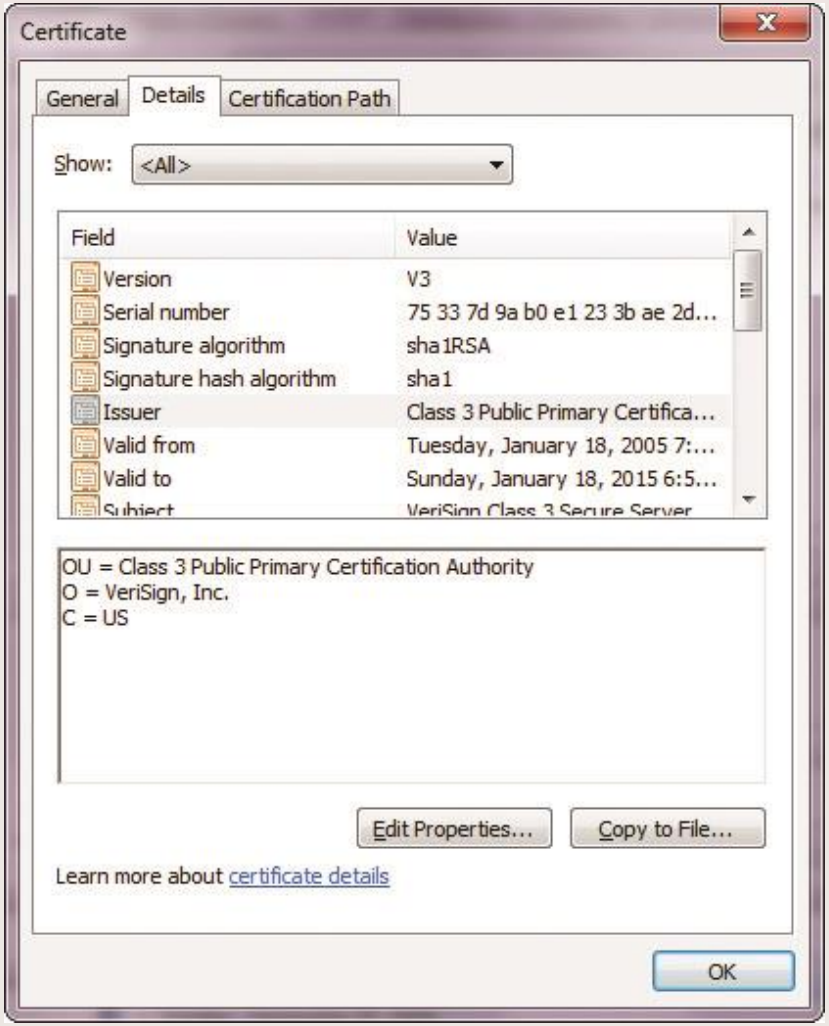
Subject Unique ID

Extension ← Other User Info, e.g., subAltName, CDP

CA Digital Signature ← Signed by CA's Private Key

- It certifies that information provided in the certificate can be trusted.

Fields Within a Digital Certificate

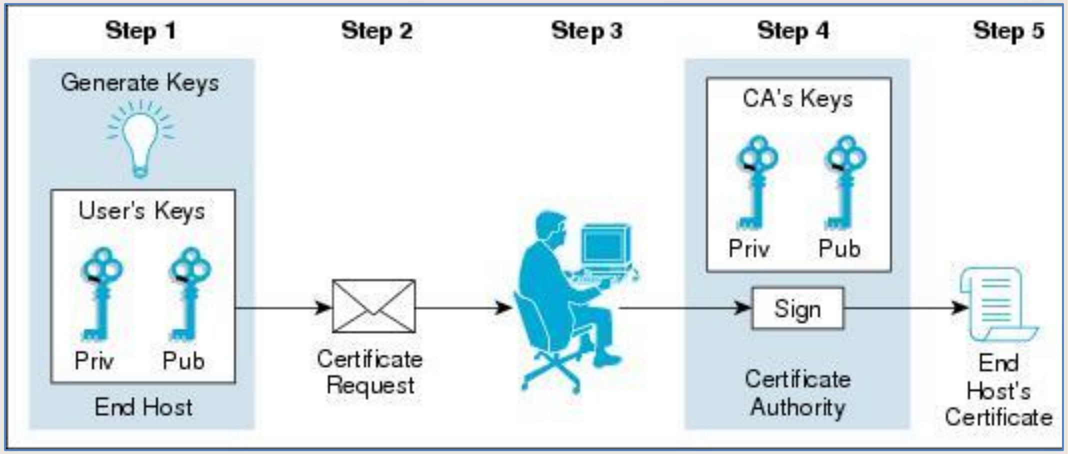


Field	Value
Version	V3
Serial number	75 33 7d 9a b0 e1 23 3b ae 2d...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	Class 3 Public Primary Certifica...
Valid from	Tuesday, January 18, 2005 7:...
Valid to	Sunday, January 18, 2015 6:5...
Subject	VeriSign Class 3 Secure Server

OU = Class 3 Public Primary Certification Authority
O = VeriSign, Inc.
C = US

Learn more about certificate details

Steps for Obtaining a Digital Certificate



- ❑ The certificate applicant must generate his/her own key pair and send the public key to the CA with some proof of his/her ID.
- ❑ The CA put the public key in a new certificate, digitally sign the certificate using its private key and then send the certificate to the applicant.

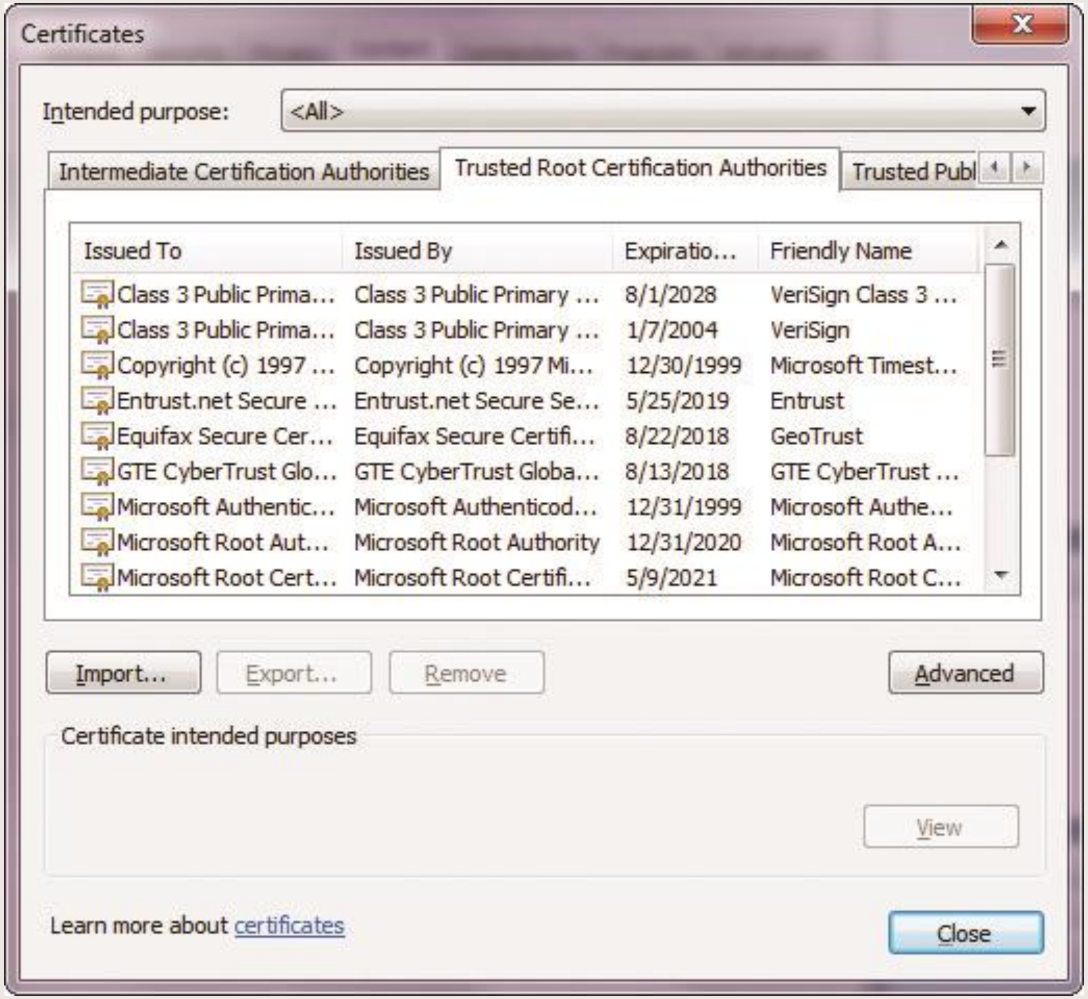
Note: The CA will check the certificate applicant's ID before it generates the certificate and signs the request.

Different CAs may issue certificates with varying levels of ID requirements. One CA may insist on seeing the ID card, another may want a signed letter authorizing certification from anyone requesting a certificate.

Trust and Certificate Verification

- ❑ Use PKI if you do not automatically trust individuals you do not know.
- ❑ A third party that is trusted by both the first and second party is needed.
- ❑ A user will trust a certificate authority and download that CA's digital certificate and public key.
- ❑ Certificate authorities you trust can be found in your browser's list.

The Browser's List of CAs



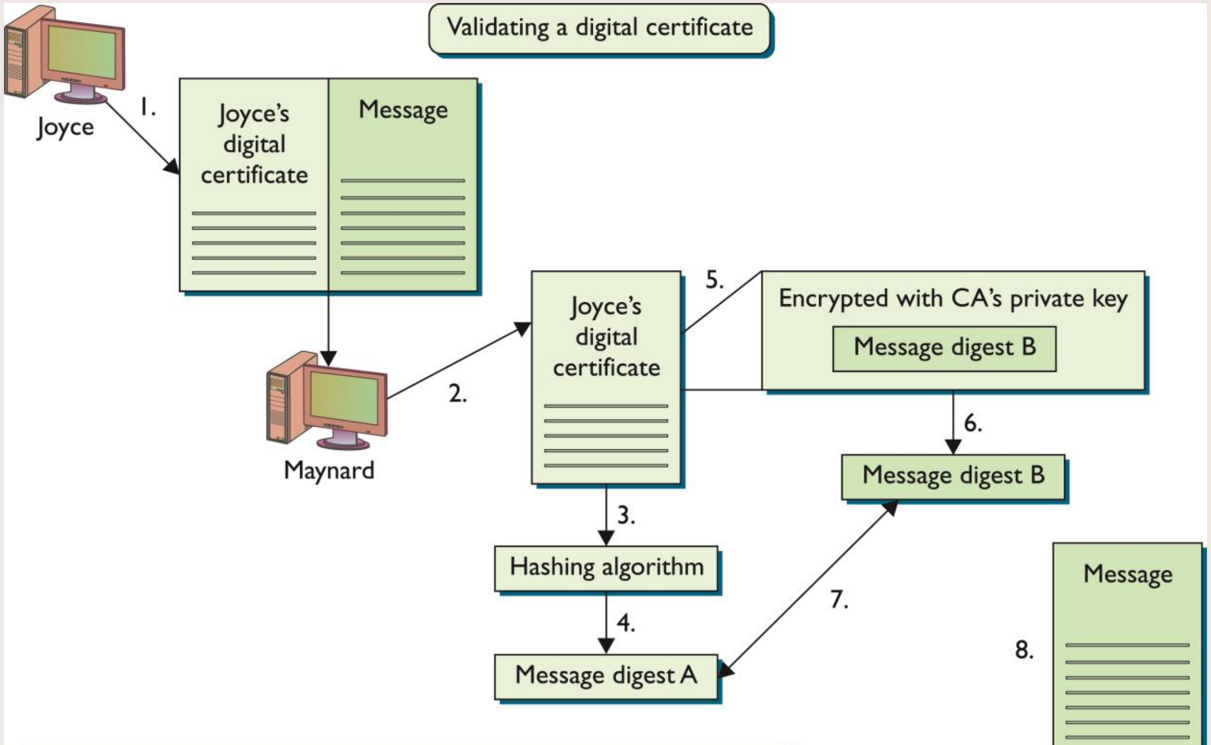
Certificates

Intended purpose: <All>

Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ

Issued To	Issued By	Expiratio...	Friendly Name
Class 3 Public Prima...	Class 3 Public Primary ...	8/1/2028	VeriSign Class 3 ...
Class 3 Public Prima...	Class 3 Public Primary ...	1/7/2004	VeriSign
Copyright (c) 1997 ...	Copyright (c) 1997 Mi...	12/30/1999	Microsoft Timest...
Entrust.net Secure ...	Entrust.net Secure Se...	5/25/2019	Entrust
Equifax Secure Cer...	Equifax Secure Certifi...	8/22/2018	GeoTrust
GTE CyberTrust Glo...	GTE CyberTrust Globa...	8/13/2018	GTE CyberTrust ...
Microsoft Authentic...	Microsoft Authenticod...	12/31/1999	Microsoft Authe...
Microsoft Root Aut...	Microsoft Root Authority	12/31/2020	Microsoft Root A...
Microsoft Root Cert...	Microsoft Root Certifi...	5/9/2021	Microsoft Root C...

Steps for Verifying a Certificate


Validating a digital certificate
Joyce
1.
Joyce's digital certificate
Message
Maynard
2.
Joyce's digital certificate
5.
Encrypted with CA's private key
Message digest B
6.
Message digest B
3.
Hashing algorithm
4.
Message digest A
7.
8.
Message

1. Joyce sends the message and digital certificate to Maynard.
2. Maynard extracts the certificate.
3. Maynard puts the certificate through a hashing algorithm.
4. The algorithm calculates a value of A.
5. Maynard extracts the encrypted message digest from the certificate.
6. Maynard decrypts the value with the CA's public key.
7. Maynard checks to see if the certificate was revoked.
   Maynard compares values A and B.
8. The values are the same, so Maynard reads the message.

Public Certificate Authorities

- ❑ Public CAs are already established and being used by many other individuals and companies.
  - ❖ Specialize in verifying individual identities and creating and maintaining their certificates
  - ❖ Issue certificates that are not bound to specific companies or departments
- ❑ Some examples of public CAs are VeriSign (including GeoTrust and Thawte), Entrust, and Go Daddy.

In-House Certificate Authorities

- ❑ An in-house *CA* is implemented, maintained, and controlled by the company that implemented it.
- ❑ This type of *CA* can be used to create certificates for internal employees, devices, applications, partners, and customers.
- ❑ The company has complete control over how individuals are identified, what certification classifications are created, who can and cannot have access to the *CA*, and how the certifications can be used.

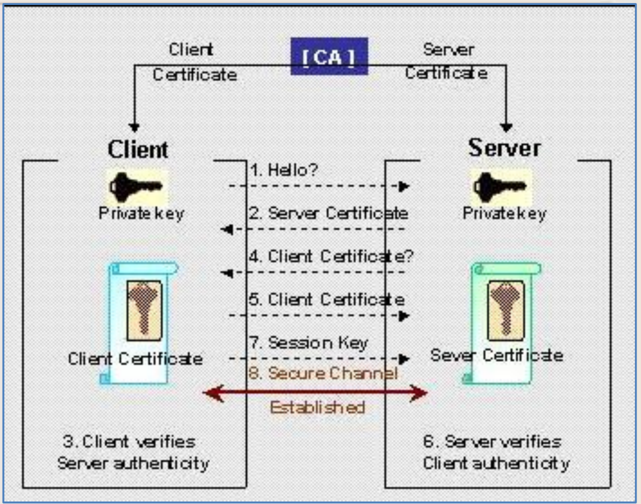
Choosing Between a Public CA & an In-House CA

- ❑ Each company is unique, and many factors must be taken into consideration.
  - ❖ It is not just a financial decision.
- ❑ Using public CAs
  - ❖ Public CAs already have the necessary equipment, skills, and technologies.
- ❑ Using in-house CAs
  - ❖ Some companies do not trust an outside authority to generate and maintain their company's certificates.

Outsourced Certificate Authorities

- Outsource different parts of it to a specific service provider.
  - The more complex parts are outsourced, such as the CA, RA, CRL, and key recovery mechanisms.
- It is used when the company does not have the necessary skills to implement and carry out a full PKI environment.
- You must determine the level of trust the company is willing to give the service provider and what level of risk it is willing to accept.

How do digital certificates work in a web site?



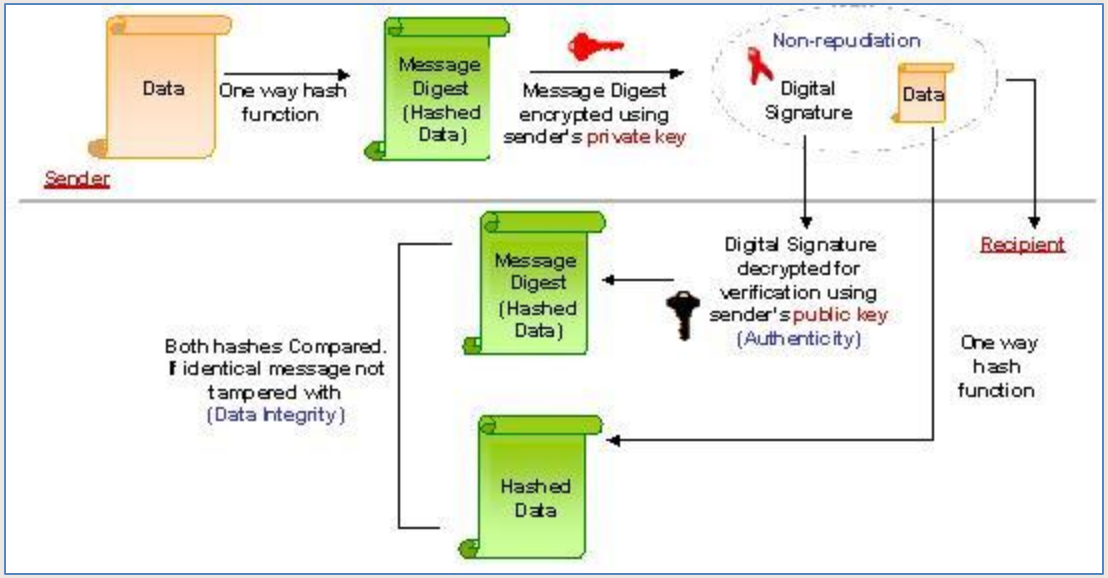
- ❑ The user visits a secure web site.
- ❑ The server send certificate to the client (browser)
- ❑ The user verifies the server authenticity to ensure that it is an exact site the user is visiting.
- ❑ The server requests a client certificate from the client.
- ❑ The user selects an appropriate certificate to present.
- ❑ The server verifies the client authenticity to ensure that it is an authorized user.
- ❑ When authentication is complete, the client sends the server a session key encrypted using the server's public key.
- ❑ A secure channel is established between the client and server

How do digital certificates work in e-mail

Sender:

❑ To send a signed data/message to the recipient.

❑ He creates a MD by using a hash function on the message.


Data
One way hash function
Message Digest (Hashed Data)
Message Digest encrypted using sender's private key
Non-repudiation
Digital Signature
Data
Sender
Recipient
Message Digest (Hashed Data)
Digital Signature decrypted for verification using sender's public key (Authenticity)
Both hashes Compared. If identical message not tampered with (Data Integrity)
One way hash function
Hashed Data

❑ Then encrypts the data/message digest with his private key.

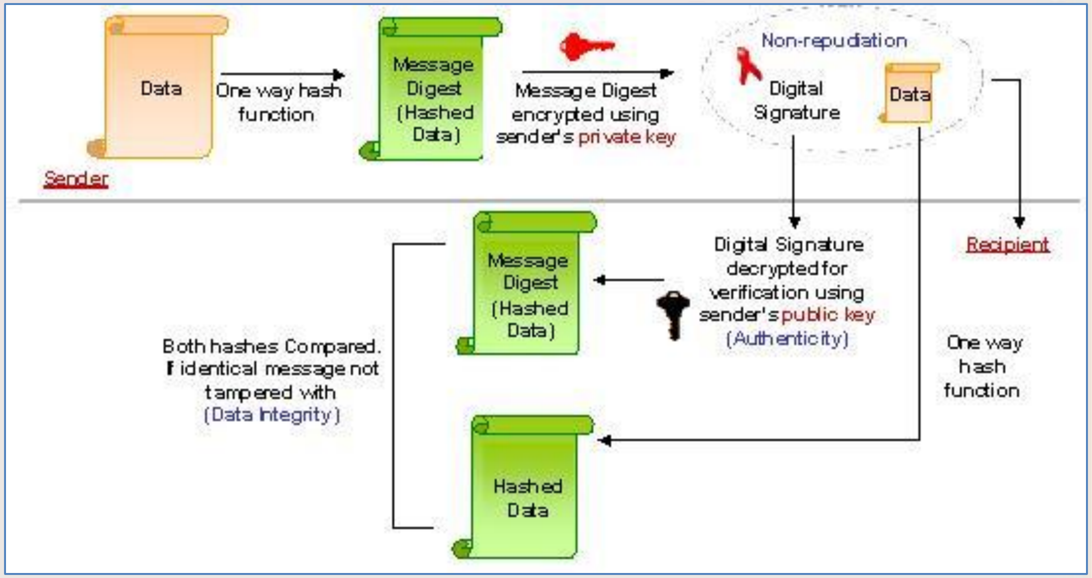
❑ This encrypted MD is called a DS and is attached to sender's original message, resulting in a signed data/message.

❑ The sender sends his signed data/message to the recipient.

How do digital certificates work in e-mail

Recipient :

- When he receives the signed data/message, he detaches sender's DS from the data/message and decrypts the signature with the sender's public key, thus revealing the MD.

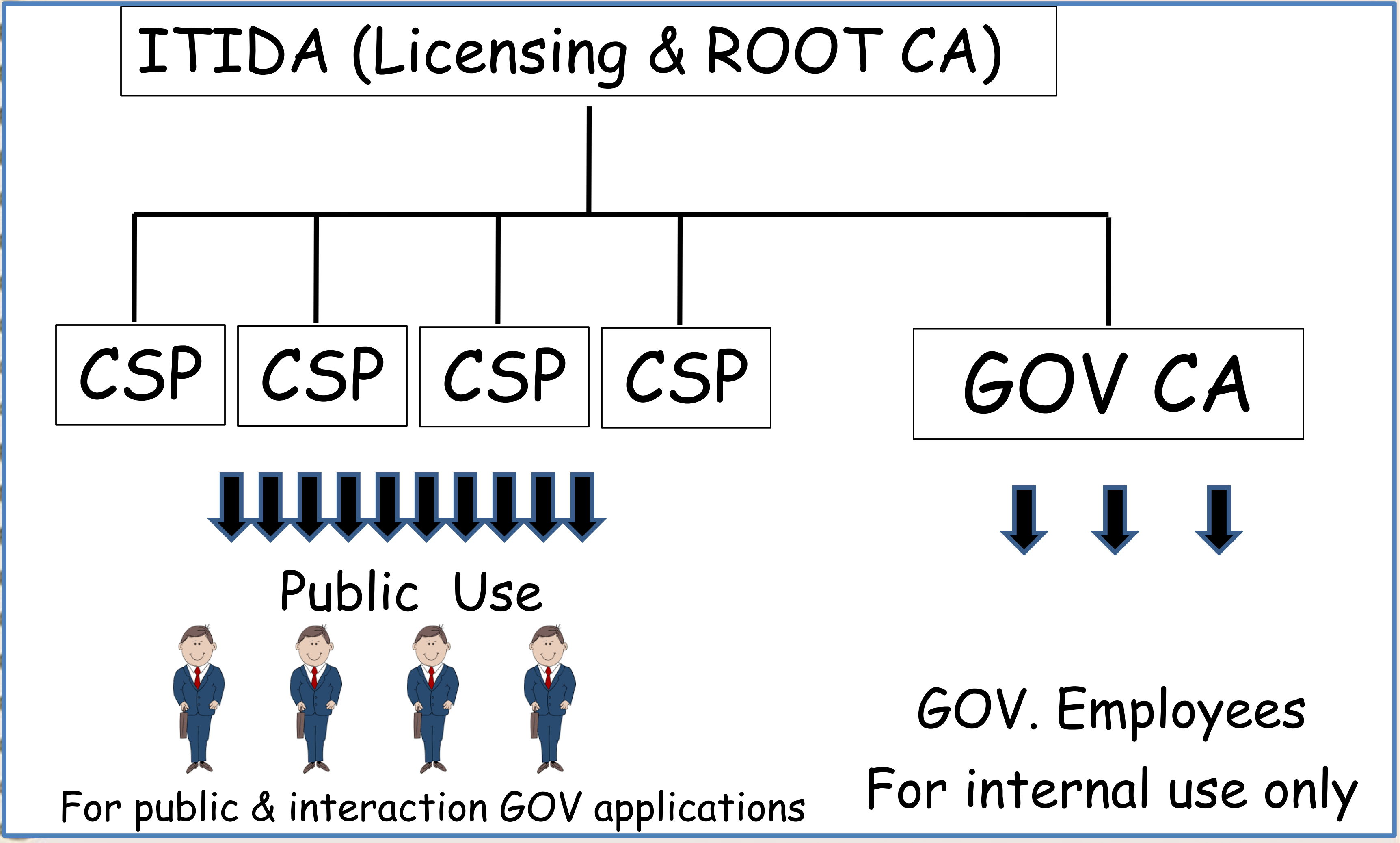

Data
One way hash function
Message Digest (Hashed Data)
Message Digest encrypted using sender's private key
Non-repudiation
Digital Signature
Data
Sender
Digital Signature decrypted for verification using sender's public key
(Authenticity)
Recipient
Message Digest (Hashed Data)
Both hashes Compared. If identical message not tampered with
(Data Integrity)
One way hash function
Hashed Data

- The data/message will be re-hashed to get the MD.
- The recipient then compares this result to the MD he receives from the sender. If they are exactly equal, the recipient can be confident that the message has come from the sender and has not changed since he signed it. If the MDs are not equal, the message may not have come from the sender of the data/message, or was altered by someone, or was accidentally corrupted after it was signed.

PKI in Egypt

- ❑ E-Signature Law issued 2004.
- ❑ Executive directives of the law issued in 2005.
- ❑ 4 CSP (certificate service providers) are licensed in 2006
- ❑ Root CA & Gov CA tendered in 2006
- ❑ Root CA started work in Sep 2009
- ❑ 1st CSP got the official permission to work in Oct. 2009
- ❑ Root CA of Egypt in ITIDA, MCIT

PKI Model in Egypt



ITIDA (Licensing & ROOT CA)

CSP

CSP

CSP

CSP

GOV CA

Public Use

For public & interaction GOV applications

GOV. Employees

For internal use only

Secure Socket Layer (SSL)

- ❑ SSL is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

- ❑ SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

- ❑ To establish SSL with web server, get SSL Certificate from CA.

- ❑ Web server will match server SSL Certificate with Private Key. Web server will then be able to establish an encrypted link between the website and user's web browser.

Secure Socket Layer (SSL)

- The SSL protocol remain invisible to the user. Instead user browser show a key indicator to let the user know he is currently protected by an SSL encrypted session - the lock icon in the lower right-hand corner, clicking on the lock icon displays site SSL Certificate and the details about it.
- Typically an SSL Certificate will contain site domain name, company name, address, city, country. It will also contain the expiration date of the Certificate and details of the CA responsible for the issuance of the Certificate.
- When a browser connects to a secure site it will retrieve the site's SSL Certificate and check that it has not expired, it has been issued by a CA the browser trusts, and that it is being used by the website for which it has been issued. If it fails on any one of these checks the browser will display a warning to the end user letting them know that the site is not secured by SSL.