Distributed Systems

COMP90015 2018 Semester 2
Tutorial 9

Things to cover today

Part 1: Project 2 Milestone Demonstration

Part 1: Security Questions

Part 2: Code Demonstration -- encrypted client and server communication

Security Questions

1. What is a digital certificate and why do we need it?
2. What is the process to obtain a digital certificate?
3. What is a certificate chain?
4. Assuming that Bob has a public/private key pair, how can Alice and Bob establish a shared key to communicate secretly using a Key Distribution Service?

What is a digital certificate and why do we need it?

- A digital certificate is a digital form of identification, like a passport.
- A digital certificate provides information about the identity of an entity.
- A digital certificate is issued by a Certification Authority (CA).
    - Examples of trusted CA across the world are Verisign, Entrust, etc.
    - The CA guarantees the validity of the information in the certificate.

- The issue of distributing Public Key is massive, because the Public Key should be distributed in a scalable and truthful way

Public Key Infrastructure (PKI)

- **Public Key Infrastructure (PKI)** consists of protocols, standards and services, that allows users to authenticate each other using digital certificates that are issued by CA. For a digital certificate to be useful, it has to be structured in a standard way so that information within the certificate can be retrieved and understood regardless of who issued the certificate. The ***X.509, PKI X.509*** and ***Public Key Cryptography Standards (PKCS)*** are the building blocks a PKI system that defines the standard formats for certificates and their use.

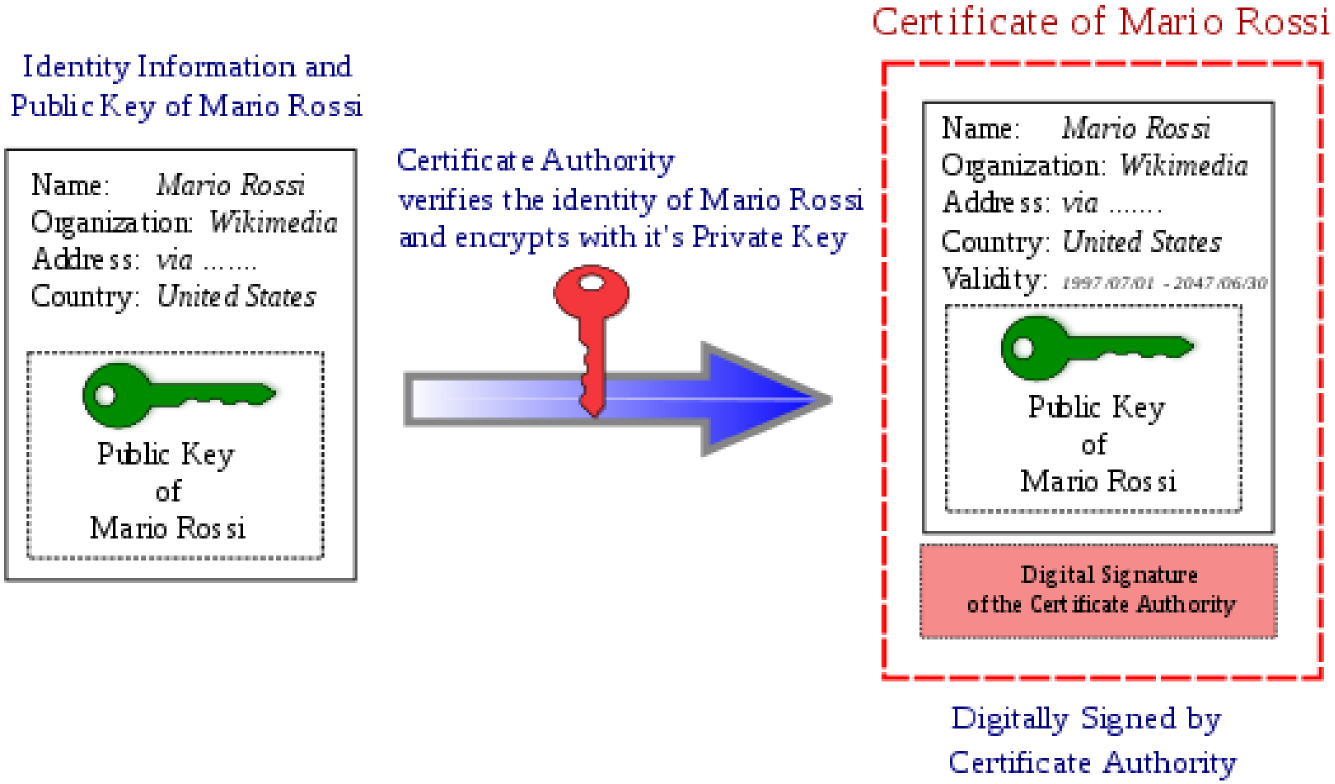
Version		Version of X.509 to which the Certificate conforms
Serial Number		A number that uniquely identifies the Certificate
Signature Algorithm ID		The names of the specific Public Key algorithms that the CA has used to sign the Certificate (Ex.- RSA with SHA-1)
Issuer (CA) X.500 Name		The identity of the CA Server who issued the Certificate
Validity Period		The period of time for which the Certificate is valid with start date and expiration date
Subject X.500 Name		The owner's identity with X.500 Directory format (Ex.- cn=auser, ou=SP, o=Alphawest)
Subject Public Key Info	Algorithm ID	The Public Key of the owner of the Certificate and the specific Public Key algorithms associated with the Public Key
	Public Key Value	
Issuer Unique ID		Information used to identify the issuer of the Certificate
Subject Unique ID		Information used to identify the Owner of the Certificate
Extension		Additional information like Alternate name, CRL Distribution Point (CDP)
CA Digital Signature		The actual digital signature of the CA

Certificates

Certificate type: Public key
Name: Bob
Public key: kBpub
Certifying authority: Sara
Signature: {Digest(field 2+field 3)}_{kSpriv}

- In your own words, what is this certificate saying?
    - Sara certifies that Bob’s public key is kBpub
- Why can’t Sara deny that she has attested to this fact?
    - Because if someone can decrypt the signature using kSpub, only someone who had kSpriv could have encrypted it.
- What must be known to anyone who wants to make sure the certificate is authentic?
    - kSpub

Public Key Certificate



Identity Information and
Public Key of Mario Rossi

Name: *Mario Rossi*
Organization: *Wikimedia*
Address: *via ....*
Country: *United States*

Public Key
of
Mario Rossi

Certificate Authority
verifies the identity of Mario Rossi
and encrypts with it's Private Key

Certificate of Mario Rossi

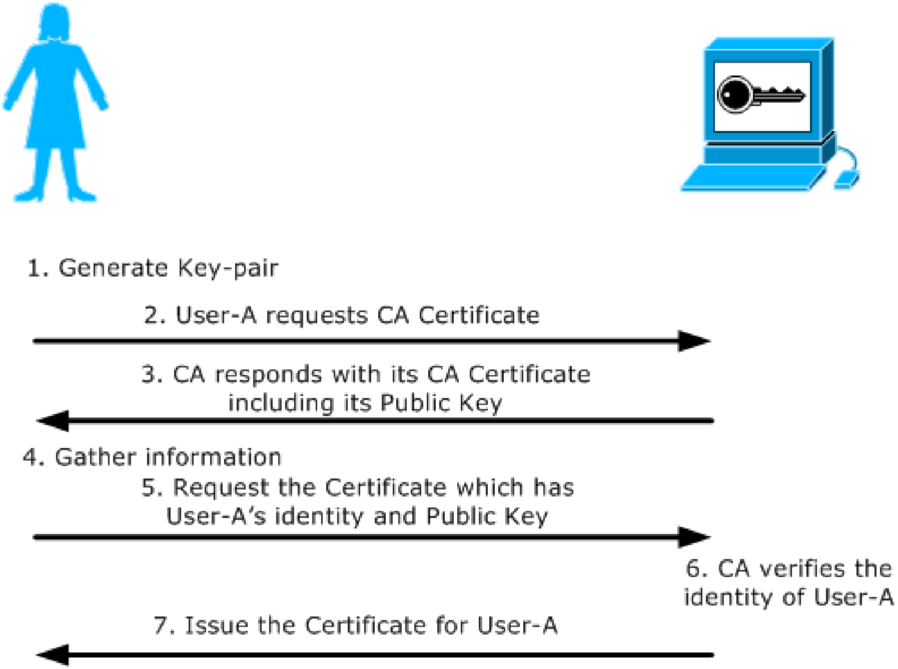
Name: *Mario Rossi*
Organization: *Wikimedia*
Address: *via ....*
Country: *United States*
Validity: *1997/07/01 - 2047/06/30*

Public Key
of
Mario Rossi

Digital Signature
of the Certificate Authority

Digitally Signed by
Certificate Authority

What is the process to obtain a digital certificate?



1. Generate Key-pair

2. User-A requests CA Certificate

3. CA responds with its CA Certificate including its Public Key

4. Gather information

5. Request the Certificate which has User-A's identity and Public Key

6. CA verifies the identity of User-A

7. Issue the Certificate for User-A

1. Generate Key-pair: User-A generates a Public and Private key-pair or is assigned a key-pair by some authority in their organization.

2. Request CA Certificate: User-A first requests the certificate of the CA Server.

3. CA Certificate Issued: The CA responds with its Certificate. This includes its Public Key and its Digital Signature signed using its Private Key.

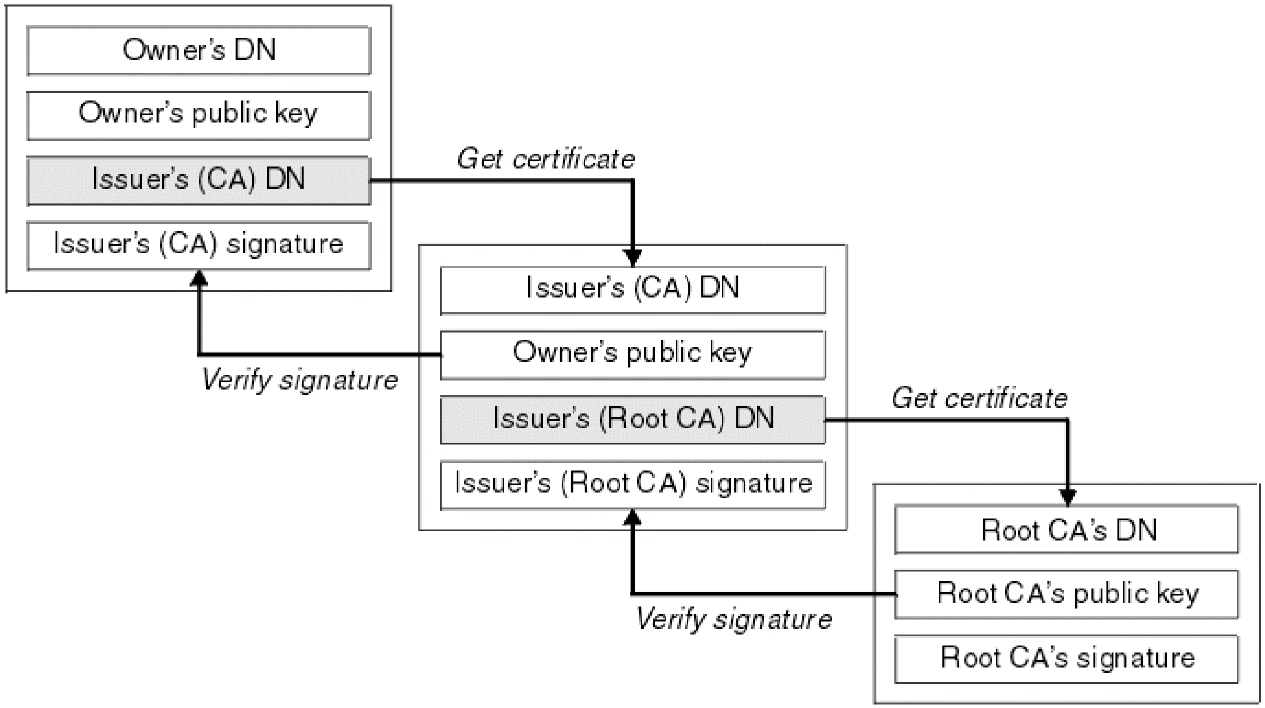
4. Gather Information: User-A gathers all information required by the CA Server to obtain its certificate. This information could include User-A email address, fingerprints, etc. that the CA needs to be certain that User-A claims to be who she is.

5. Send Certificate Request: User-A sends a certificate request to the CA consisting of her Public Key and additional information. The certificate request is signed by CA's Public Key.

6. CA verifies User-A: The CA gets the certificate request, verifies User-A's identity and generates a certificate for User-A, binding her identity and her Public Key. The signature of CA verifies the authenticity of the Certificate.

7. CA issues the Certificate: The CA issues the certificate to User-A.

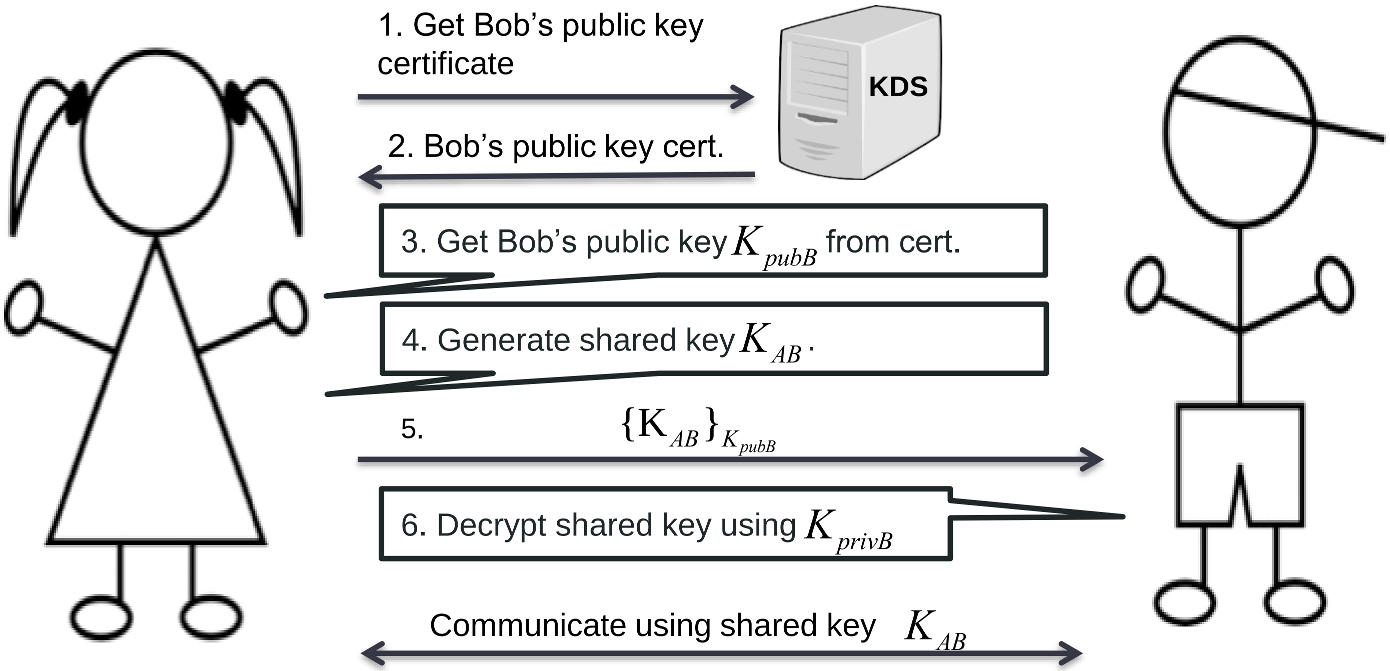
What is a certificate chain?



Example usage of certificate chain

- During a User's certificate validation by a browser or a program, browser needs to validate the signature by finding the public key of the next issuing CA or intermediate CA. The process will continue until the root certificate is reached. Root CA is self signed and must be trusted by the browser at the end. Browsers keep all well known CAs root certificates in their trust store.

Assuming that Bob has a public/private key pair, how can Alice and Bob establish a shared key to communicate secretly using a Key Distribution Service?



1. Get Bob's public key certificate

2. Bob's public key cert.

3. Get Bob's public key K_{pubB} from cert.

4. Generate shared key K_{AB}.

5. $\{K_{AB}\}_{K_{pubB}}$

6. Decrypt shared key using K_{privB}

Communicate using shared key K_{AB}

Code Demonstration