Distributed Systems

COMP90015 2023 Semester 1
Tutorial 09

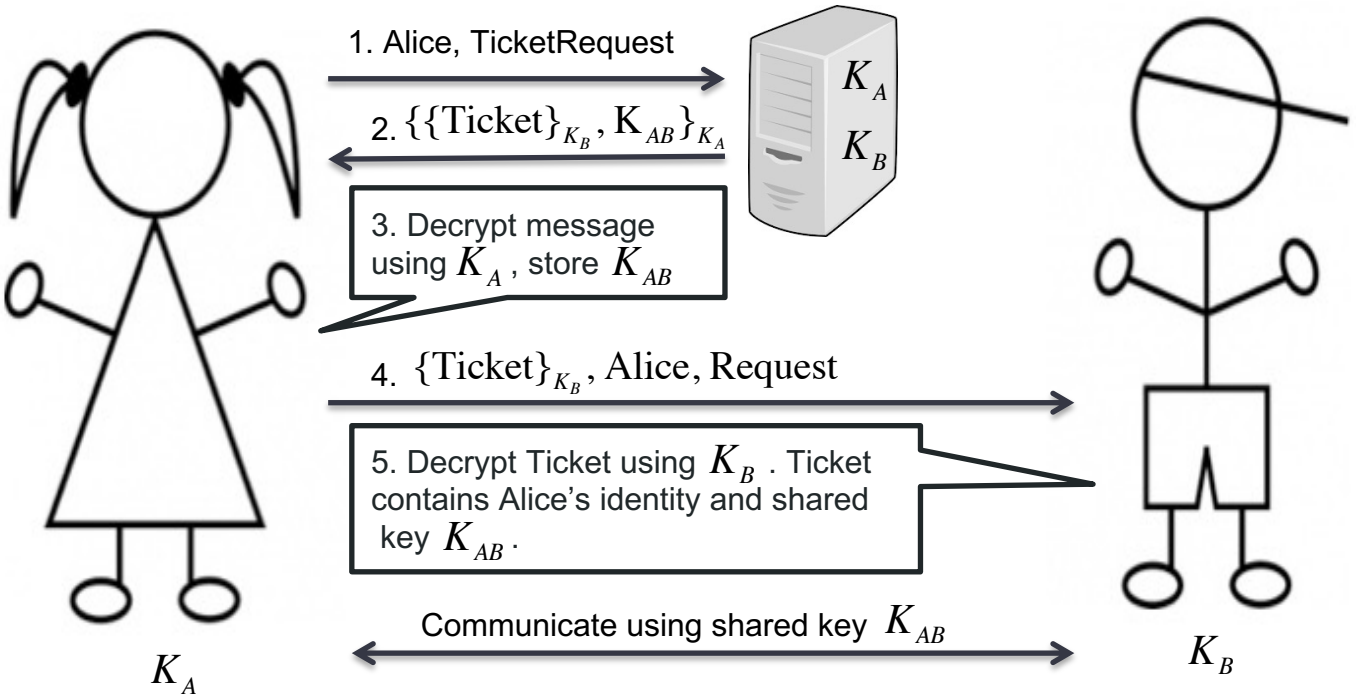
Today’s Agenda

- Assignment 2 Q & A
- Questions on Security (continued)
- Demo - Client Server Encryption

Assignment 2 Q & A

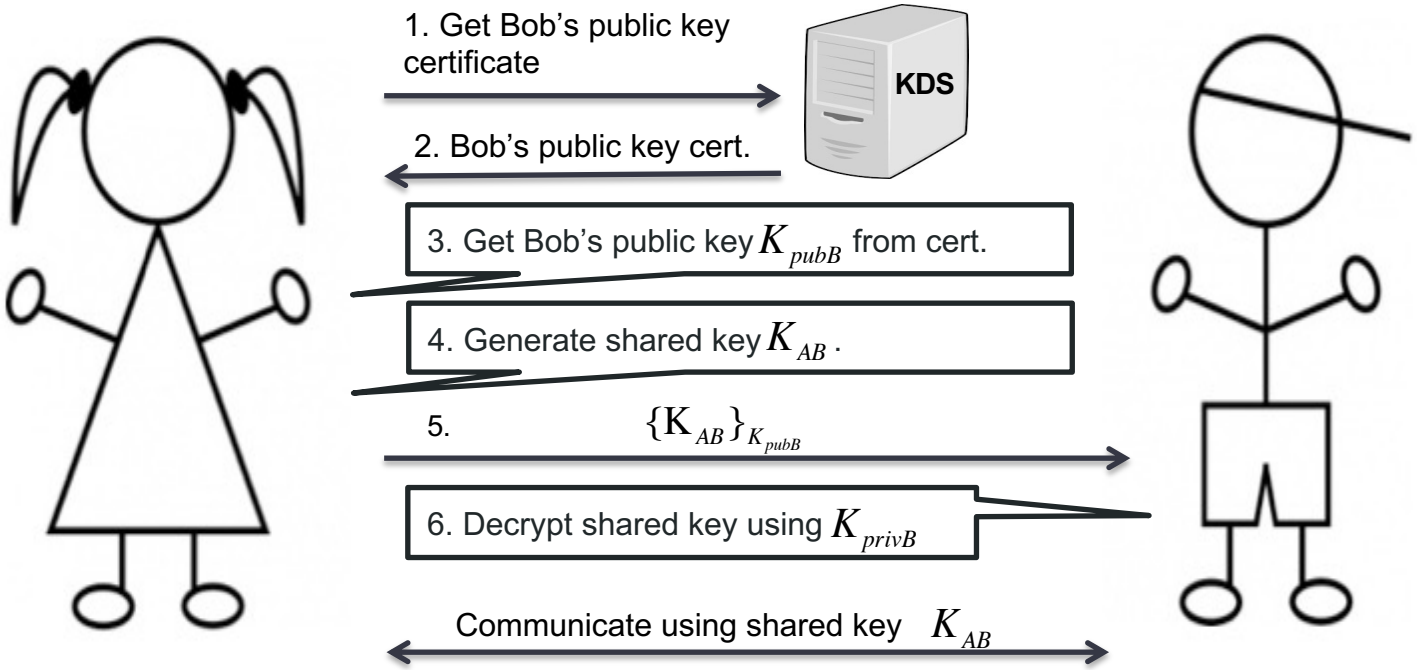
1. How can Alice authenticate and communicate secretly with Bob assuming there is an authentication server that knows Alice’s and Bob’s secret keys?

1. How can Alice authenticate and communicate secretly with Bob assuming there is an authentication server that knows Alice's and Bob's secret keys?



2. 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?

2. 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?

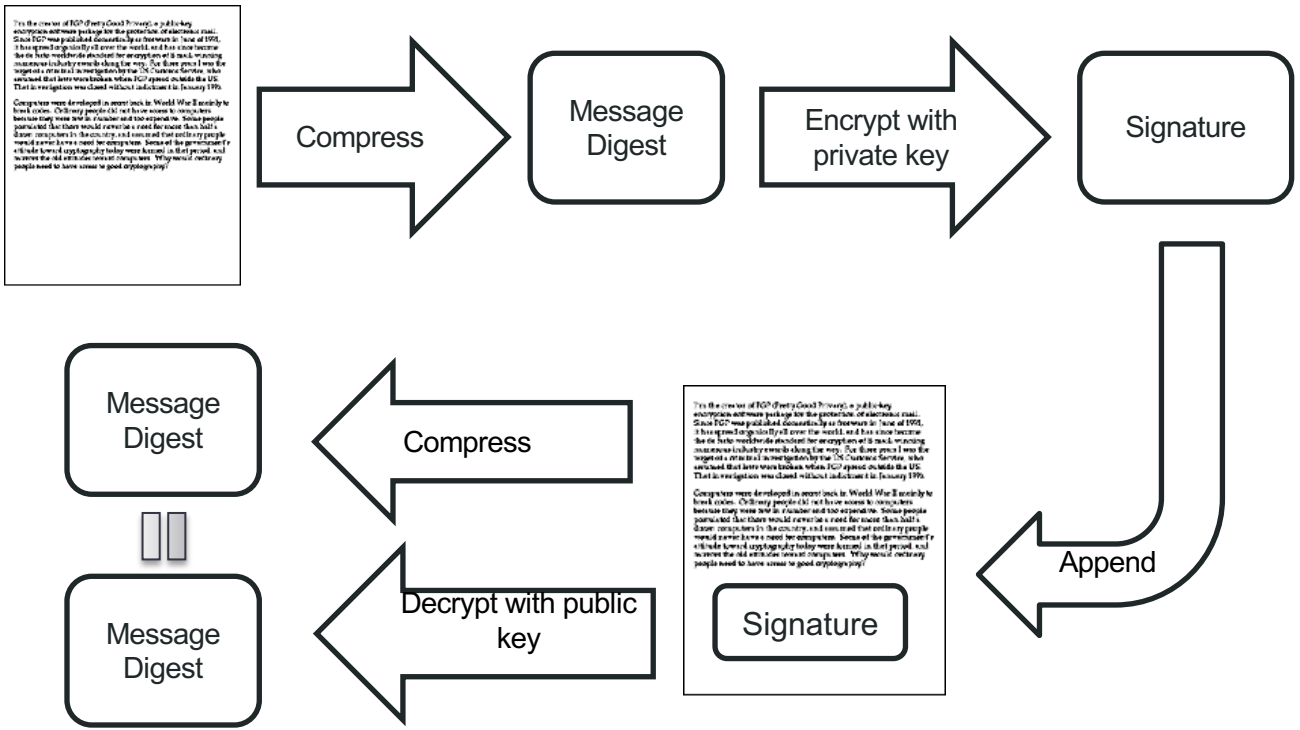


3. Explain how digital signatures work.

3. Explain how digital signatures work.

1. To sign a document, Bob first ‘compresses’ the message into just a few lines. This is called a ***digest***.
2. Bob then encrypts the message digest with his private key. The result is the **digital signature.**
3. Bob appends the digital signature to the document. All of the data that was ‘compressed’ into the digest has been signed.
4. Bob sends the document to Alice.
5. Alice decrypts the signature (using Bob's public key) changing it back into a message digest.
6. Alice ‘compresses’ the document data into a message digest. If the message digest is the same as the message digest created when the signature was decrypted, then Alice knows that the signed data has not been changed and that Bob signed the document (because only Bob has his private key)

3. Explain how digital signatures work.



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

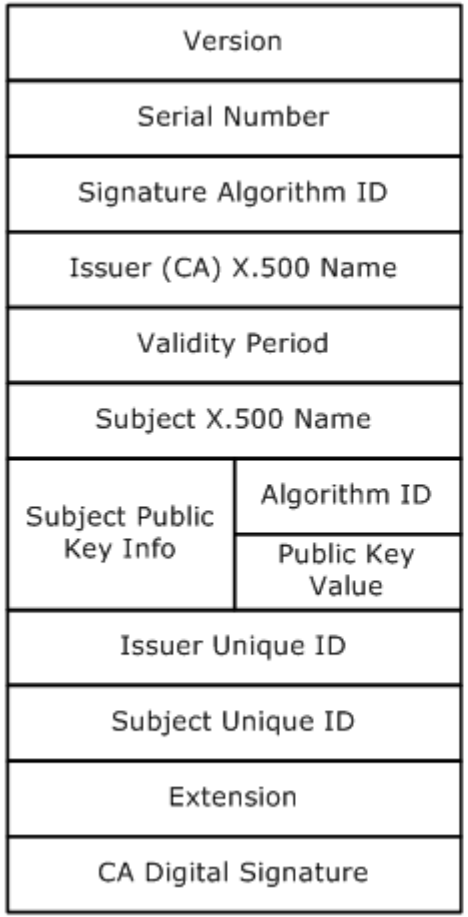
4. What is a digital certificate and why do we need it?

- 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 of X.509 to which the Certificate conforms

A number that uniquely identifies the Certificate

The names of the specific Public Key algorithms that the CA has used to sign the Certificate (Ex.- RSA with SHA-1)

The identity of the CA Server who issued the Certificate

The period of time for which the Certificate is valid with start date and expiration date

The owner's identity with X.500 Directory format (Ex.- cn=auser, ou=SP, o=Alphawest)

The Public Key of the owner of the Certificate and the specific Public Key algorithms associated with the Public Key

Information used to identify the issuer of the Certificate

Information used to identify the Owner of the Certificate

Additional information like Alternate name, CRL Distribution Point (CDP)

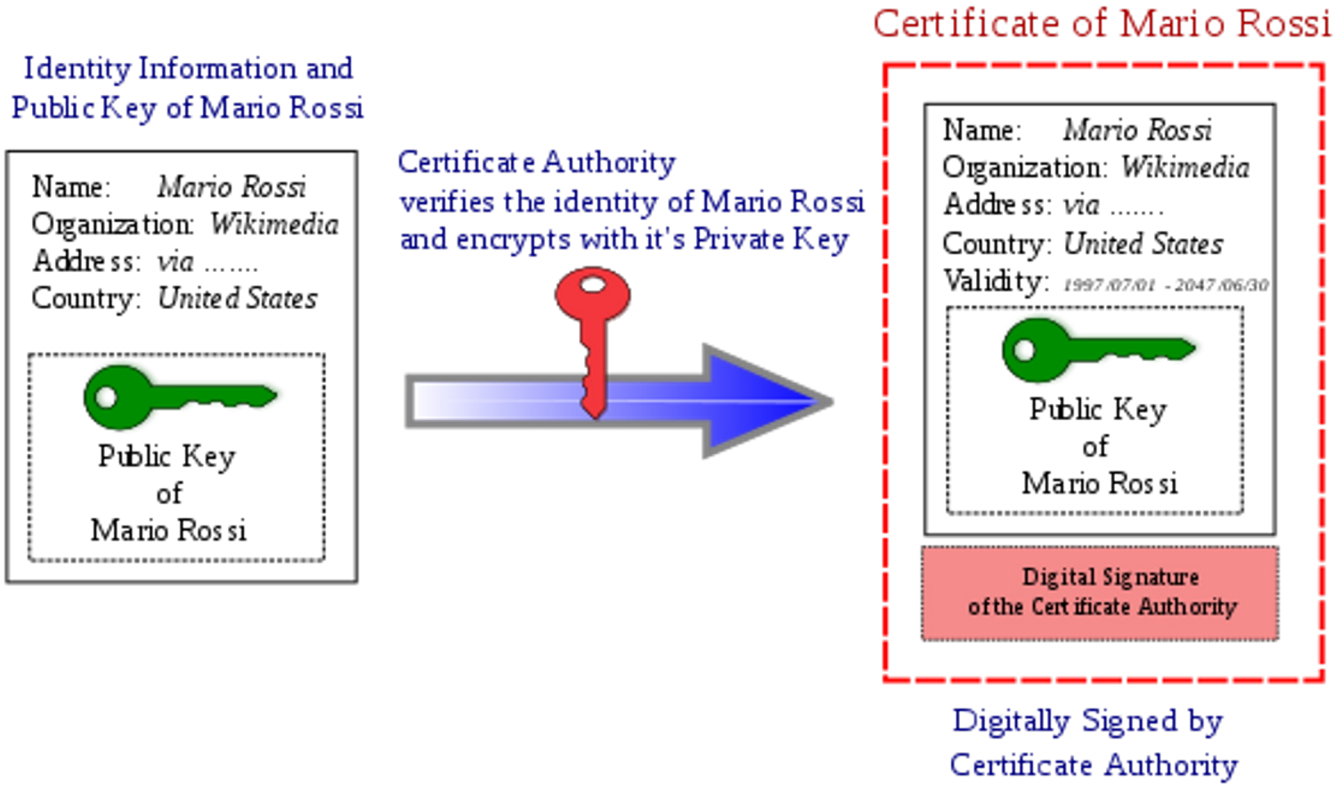
The actual digital signature of the CA

Certificates

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

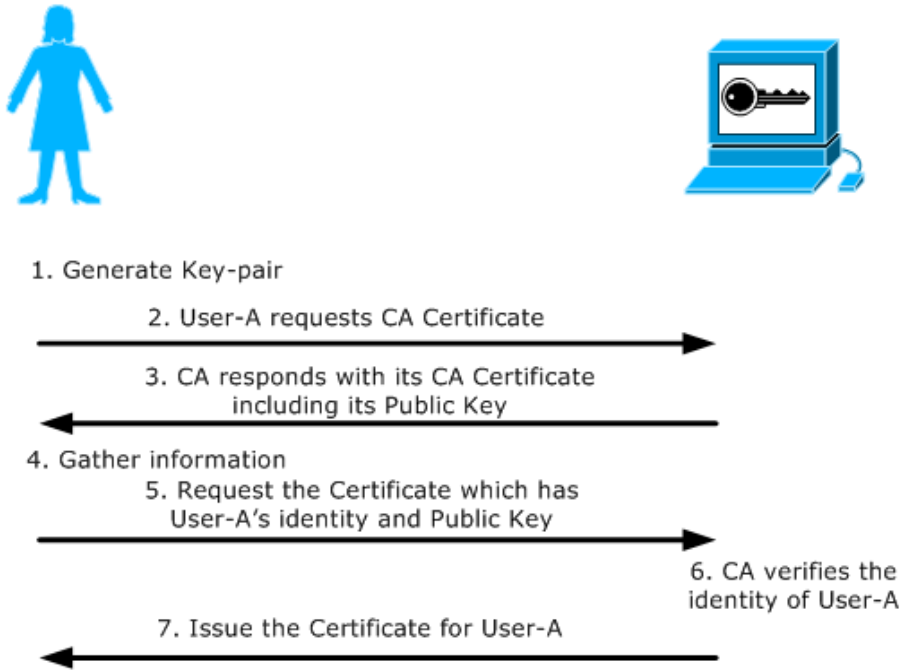
- In your own words, what is this certificate saying?
  - Sara certifies that Bob's public key is kBpub
- Why can't Sara deny that she has attested to this fact?
  - Because if someone can decrypt the signature using kSpub, only someone who had kSpriv could have encrypted it.
- What must be known to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

Public Key Certificate



5. What is the process to obtain a digital certificate?

5. What is the process to obtain a digital certificate?



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.

Code Demo

- Client Server Encryption with AES (Shared Secret Key)