DIGITAL CERTIFICATES

Dr. Shariq Mahmood Khan

shariq@cloud.neduet.edu.pk

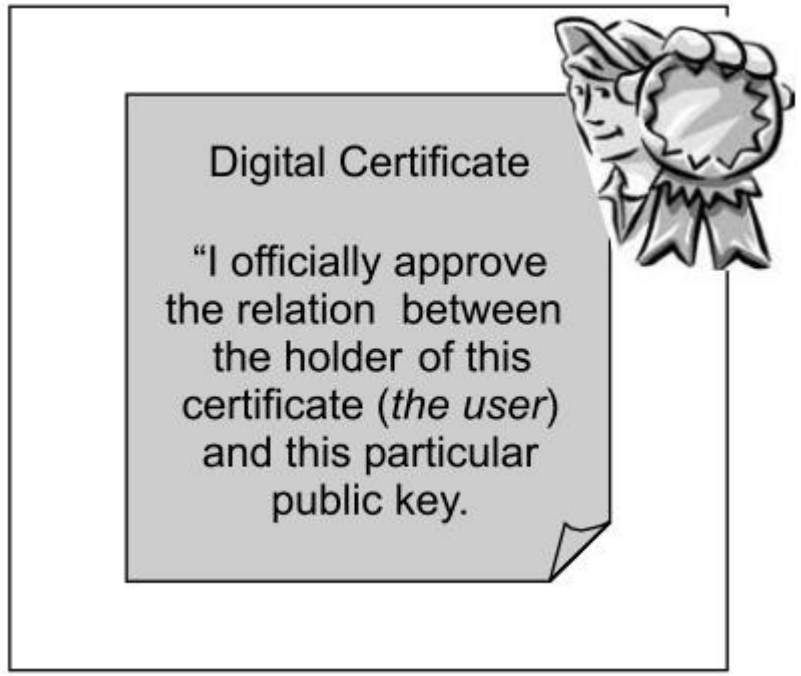
Department of Computer Science & IT, NED University of Engineering & Technology, Karachi

The Concept of Digital Certificates

- A digital certificate is simply a small computer file.
  - For example, my digital certificate would actually be a computer file with a file name such as SMK.cer (where .cer signifies the first three characters of the word certificate. Of course, this is just an example: in actual practice, the file extensions can be different.)

- Just as my passport signifies the association between me and my other characteristics such as my full name, nationality, date and place of birth, photograph and signature.

- My digital certificate simply signifies the association between my public key and me.



Conceptual view of a digital certificate

Note that this is merely a conceptual view, and does not depict the actual contents of a digital certificate.

Certification Authority (CA)

- A Certification Authority (CA) is a trusted agency that can issue digital certificates.

Who can be a CA?

- The authority of acting as a CA has to be with someone who everybody trusts.
- The governments in various countries decide who can and who cannot be a CA.
- Two of the world's most famous CAs are VeriSign and Entrust.

Digital-Certificate Creation

1. Parties Involved

a. Certification Authority(CA)

- Issuing new certificates
- Maintaining the old ones
- Revoking the ones that have become invalid for whatever reason

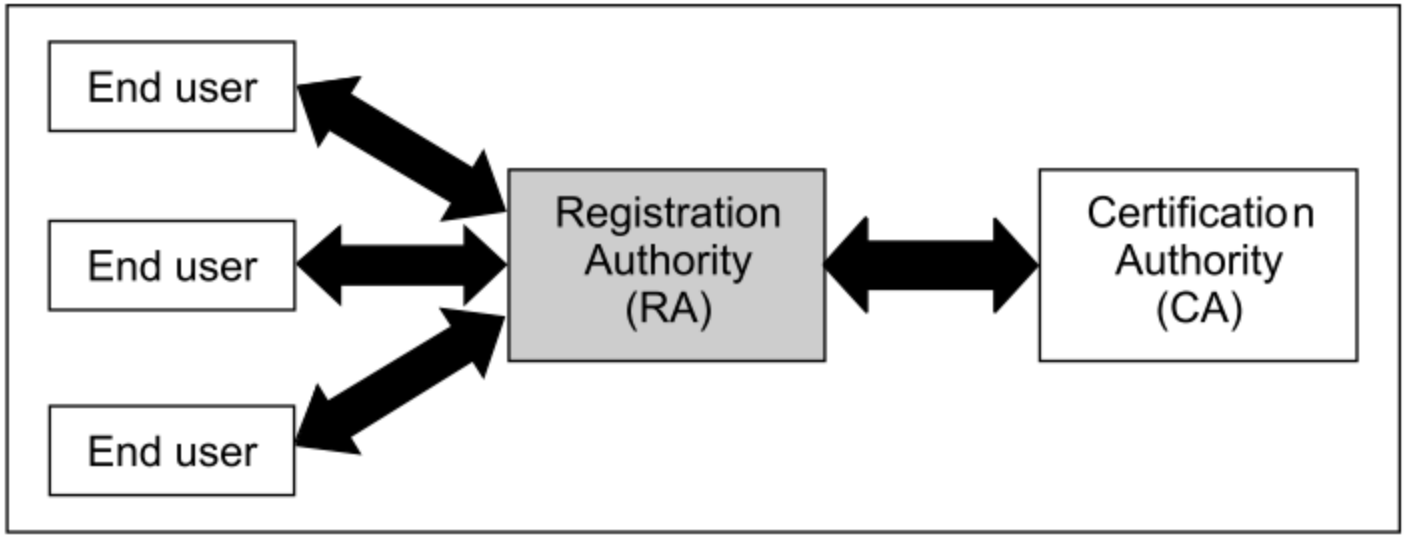
b. End User

c. Registration Authority(RA) – Optionally involved

- Accepting and verifying registration information about new users
- Generating keys on behalf of the end users
- Accepting and authorizing requests for key backups and recovery
- Accepting and authorizing the requests for certificate revocation

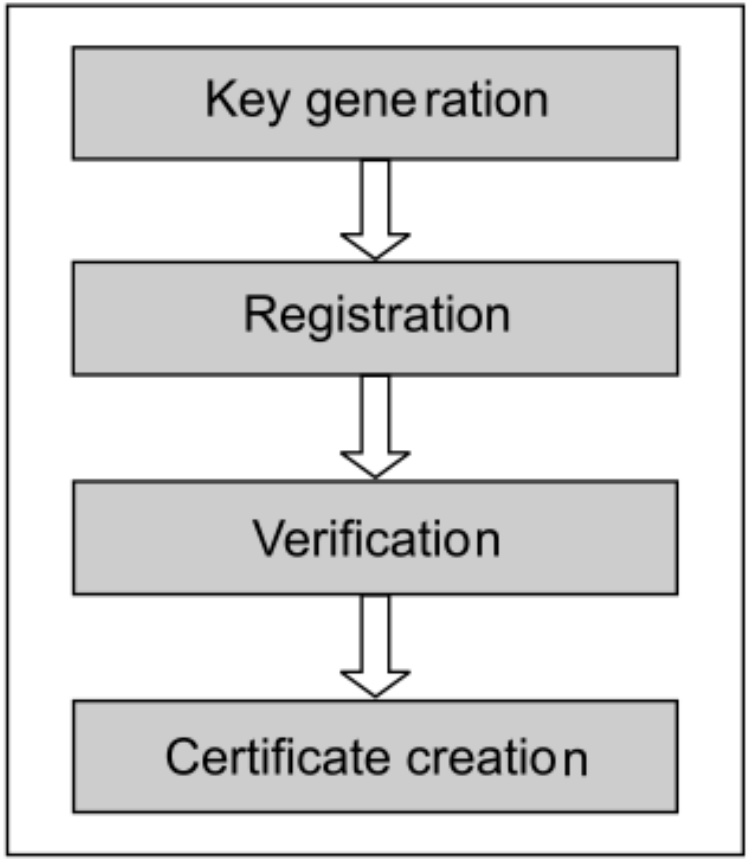
Digital-Certificate Creation

1. Parties Involved (cont.)



Digital-Certificate Creation

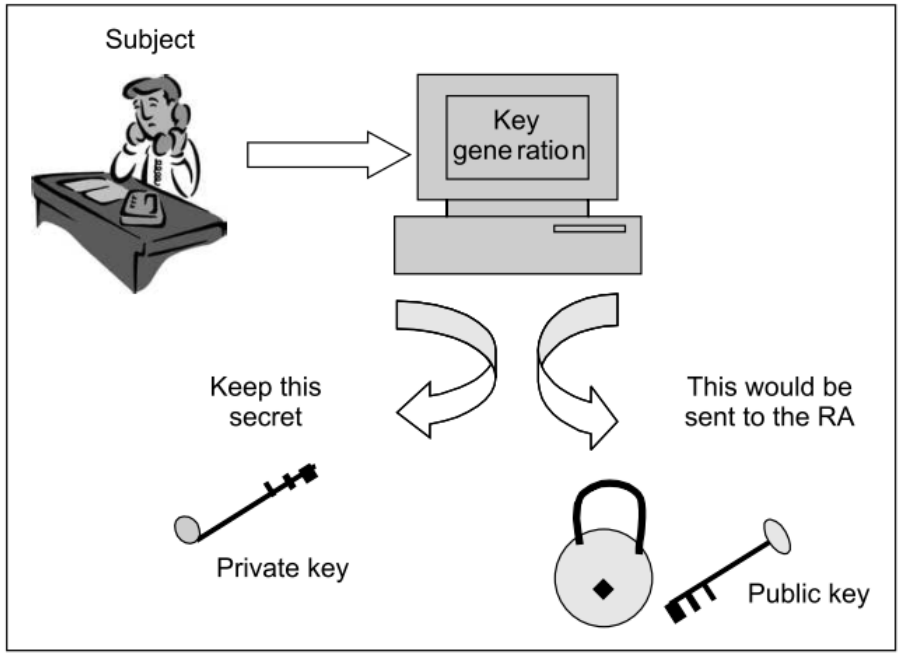
2. Certificate Creation Steps



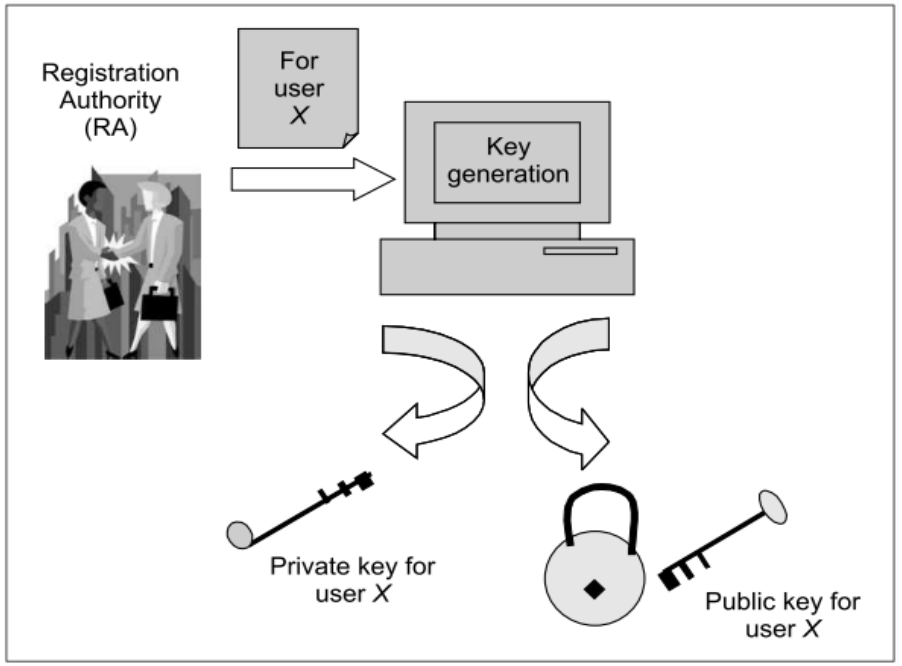
Certificate Creation Steps

Step 1: Key Generation

- The action begins with the subject (i.e. the user/organization) who wants to obtain a certificate. There are two different approaches for this purpose:
  - The subject can create a private key and public key pair using some software.
  - The RA can generate a key pair on the subject's (user's) behalf.



Subject generating its own key pair



RA generating a key pair on behalf of the subject

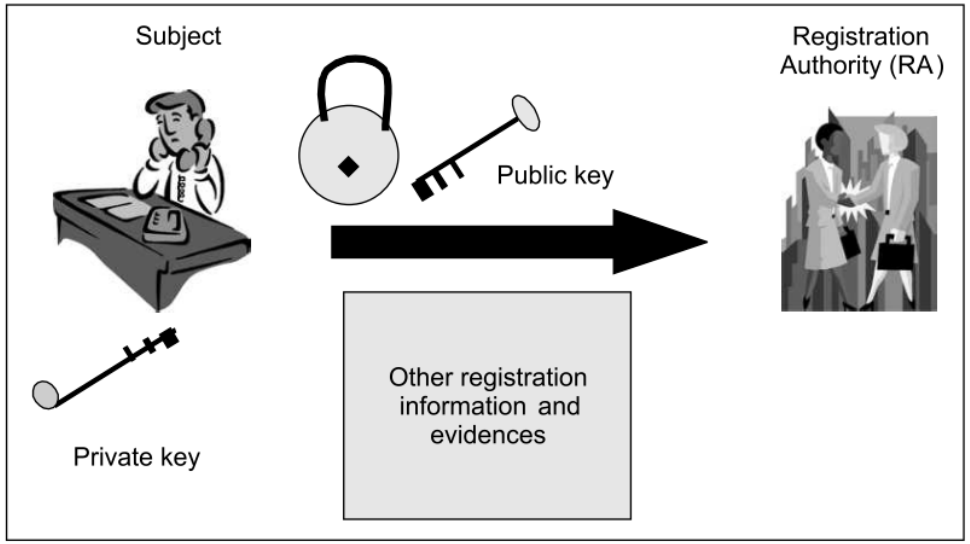
Certificate Creation Steps

Step 2: Registration

- This step is required only if the user generates the key pair in the first step. If the RA generates the key pair on the user's behalf, this step will also be a part of the first step itself.

- **Assuming that the user has generated the key pair:**

  - The user now sends the public key and the associated registration information (e.g. subject name, as it is desired to appear in the digital certificate) and all the evidence about herself to the RA.
  - The software provides a wizard in which the user enters data and when all data is correct, submits it.
  - The format for the certificate requests has been standardized, and is called Certificate Signing Request (CSR).
  - This is one of the Public Key Cryptography Standards (PKCS). CSR is also called PKCS#10.



Subject sends public key and evidences to the RA

Certificate Creation Steps

Step 3: Verification

- After the registration process is complete, the RA has to verify the user's credentials. This verification is in two respects

    a) Firstly, the RA needs to verify the user's credentials such as the evidences provided are correct, and that they are acceptable.

    b) The second check is to ensure that the user who is requesting for the certificate does indeed possess the private key corresponding to the public key that is sent as a part of the certificate request to the RA.

    This is very important, because there must be a record that the user possesses the private key corresponding to the given public key. This check is called checking the **Proof Of Possession (POP)** of the private key.

Certificate Creation Steps

Step 3: Verification (cont.)

- **How can the RA perform POP check?**

a) The RA can demand that the user must digitally sign his/her Certificate Signing Request (CSR) using his/her private key. If the RA can verify the signature (i.e. de-sign the CSR) correctly using the public key of the user, the RA can believe that the user indeed possesses the private key.

a) Alternatively, at this stage, the RA can create a random number challenge, encrypt it with the user's public key and send the encrypted challenge to the user. If the user can successfully decrypt the challenge using his/her private key, the RA can assume that the user possesses the right private key.

a) The RA can actually generate a dummy certificate for the user, encrypt it using the user's public key and send it to the user. The user can decrypt it only if he/she can decrypt the encrypted certificate, and obtain the plain-text certificate.

Certificate Creation Steps

Step 4: Certificate Creation

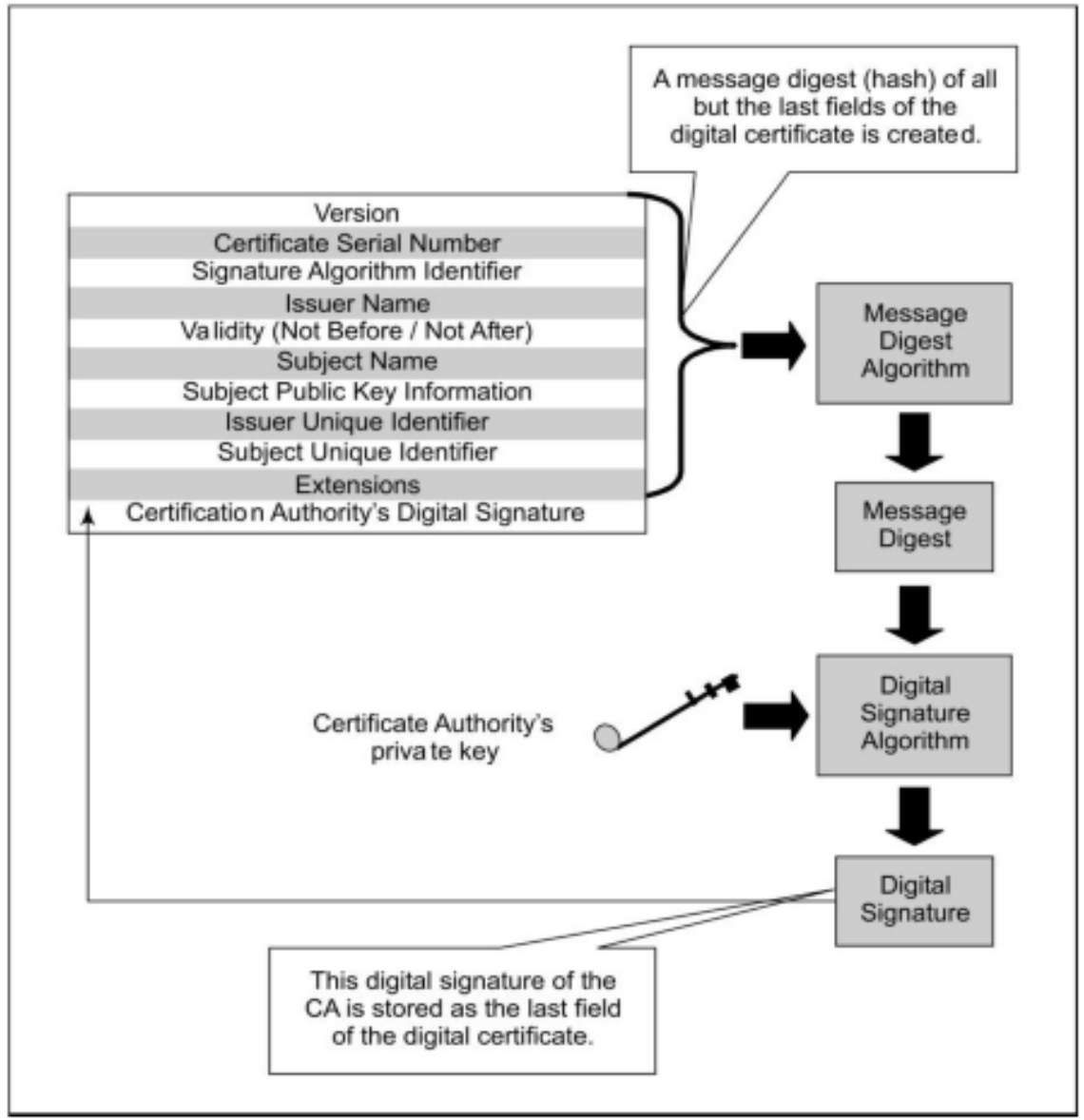
- The RA passes on all the details of the user to the CA.
- The CA does its own verification (if required) and creates a digital certificate for the user.
- There are programs for creating certificates in the X.509 standard format.
- The CA sends the certificate to the user, and also retains a copy of the certificate for its own record.
- The CA's copy of the certificate is maintained in a certificate directory.
- This is a central storage location maintained by the CA.
- The contents of the certificate directory are similar to that of a telephone directory.
- This facilitates for a single-point access for certificate management and distribution.

How a CA Signs a Certificate

- The last field in a digital certificate is always the digital signature of the CA. That is, every digital certificate not only contains the user's information (such as subject name, public key, etc.) but also the CA's digital signature. Like a passport, therefore, a digital certificate is always signed or certified.

- The CA first calculates a message digest over all the fields of the certificate (using a standard message-digest algorithm such as MD5 or SHA-1) and then encrypts the message digest with its private key (using an algorithm such as RSA) to form the CA's digital signature.

- The CA then inserts its digital signature thus calculated, as the last field in the digital certificate of the user. This is very similar to how an authority embosses, stamps and signs a passport after it is ready.



How a Digital Certificate can be Verified

The verification of a digital certificate consists of the following steps.

a) The user passes all fields except the last one of the received digital certificate to a message-digest algorithm This algorithm should be the same as the one used by the CA while signing the certificate. The CA mentions the algorithm used for signing along with the signature in the certificate, so the user here knows which algorithm is to be used.
b) The message-digest algorithm calculates a message digest (hash) of all fields of the certificate, except for the last one. Let us call this message digest as MD1.
c) The user now extracts the digital signature of the CA from the certificate (remember, it is the last field in a certificate).

How a Digital Certificate can be Verified

a) The user de-signs the CA's signature (i.e. the user decrypts the signature with the CA's public key).

b) This produces another message digest, which we shall call MD2. Note that MD2 is the same message digest as would have been calculated by the CA during the signing of the certificate (i.e. before it encrypted the message digest with its private key to create its digital signature over the certificate).

c) Now, the user compares the message digest it calculated (MD1) with the one, which is the result of de-signing the CA's signature (MD2). If the two match, i.e. if MD1 = MD2, the user is convinced that the digital certificate was indeed signed by the CA with its private key. If this comparison fails, the user will not trust the certificate, and reject it.

How a Digital Certificate can be Verified