

Assignment

classmate

Date _____

Page _____

Name: Abhirab Mukharjee

Enrolment No.: 510519109

Q1) why should we trust digital certificate?

→ Digital Certificates are made to signify that the association between ~~the~~ a public key and it's owner is legitimate and is not false.

→ We should trust digital certificates as ~~they have~~ the public key and corresponding owner has been tested for it's authenticity by trusted Certification Authorities (CA) like Verisign & Entrust.

Q2) How does CA sign a digital certificate?

→ given that an ^{end} user ~~gives~~ wants to get a digital certificate for his/her public key, the Certification Authorities tests the person and corresponding public key with a "proof of possession" test.

→ This test can be done in two ways

- (i) → End User gives two things to the Certification Authority
 - (a) His/Her public key
 - (b) His/her public key, but in cipher text form encrypted by his/her private key

→ The CA decrypts the ciphertext and checks that the decrypted plaintext match with the public key.

- (ii) → User sends his/her public key to CA, CA encrypts some data with it and gives it back to user
- User then decrypts the ciphertext and gives decrypted data back to CA
- Both ~~data~~ original data and decrypted data should match for passing the test

★ → After Verification, The CA signs the certificate in following way

- (i) Add basic details like owner, his public key, issuer, expiry date etc
- (ii) Encrypt it using CA's private key
- (iii) append CA's digital certificate to the cipher text

→ Now the digital certificate is signed with CA's authentic ~~key~~ public key.

(Q3) How can we verify a digital certificate?

→ If a user wants to verify a digital certificate, he/she can follow the following steps

- (i) pass all fields except last one (Digital signature of Certification Authority) to a message-digest algorithm. We have to use the same message-digest algorithm the CA used, which can be easily found out via Internet ~~for this~~ (CA itself documents this)
- (ii) The message-digest algorithm calculates the hash, let this hash be MD_1
- (iii) Now we extract digital signature of CA from the last parameter and using it find the public key of CA
- (iv) We now decrypt the remaining field of certificate using public key of CA
- (v) let the digests inside the decrypted message be MD_2

→ if $MD_1 = MD_2$, then we can confirm that the digital certificate is issued by the CA.