Feedback on Topic 7 Ex

Exercise Question – E7.1(i)

(i) Investigate an on-line CA and find out what process or procedures that are necessary for you to acquire a public key certificate, how many classes of certificates and what each class can be used for.

A: Answer to this question is dependent on a particular PKI or CA.

Exercise Question – E7.1(ii)

(ii) X.509 is a top-down approach to public key management. Investigate and describe a bottom-up approach to public key management.

Exercise Question – E7.1(ii) - A

Assumption: You knows A, B, C, D, E, F.

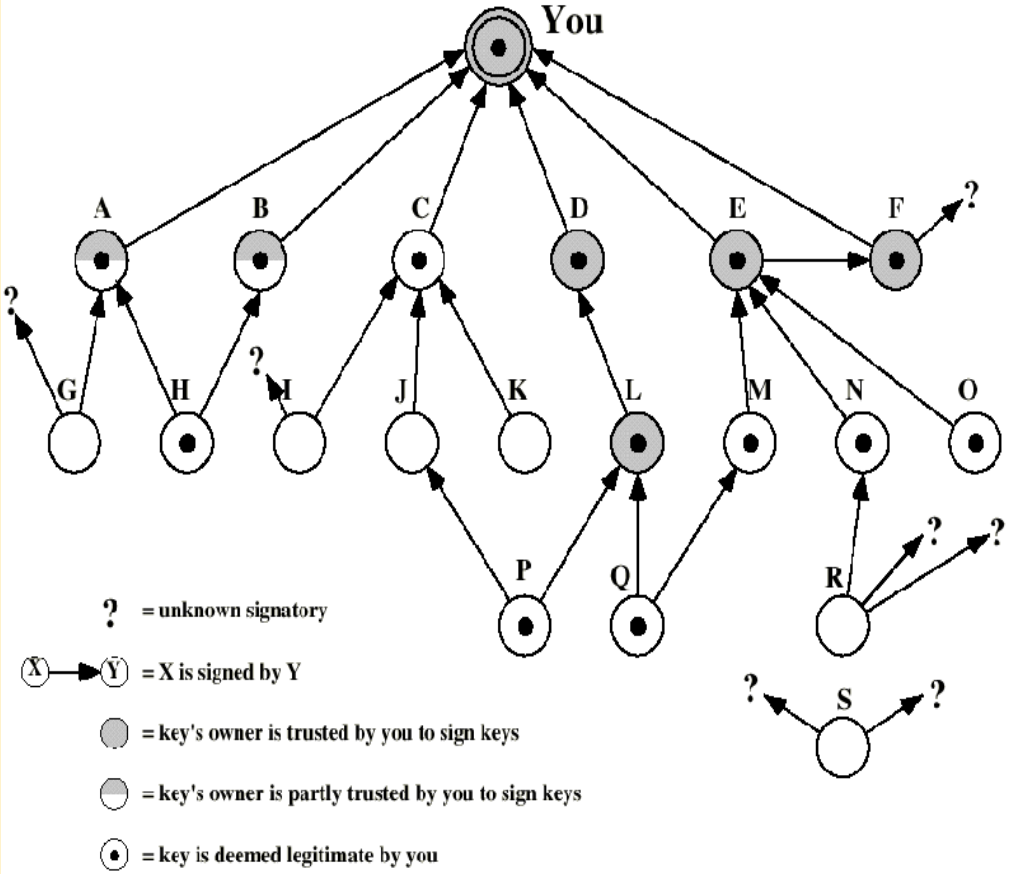
Let us say H wants to communicate with You, You do not know H, but You know A and B, and A and B know H. So A and B can sign H's public key.

If A and B are fully trusted by You, then one signature (on H's public key), either from A or B, would be sufficient.

However, if A and B are partially trusted by You, then signatures from both A and B may be necessary.

You can use other heuristics, e.g. if You gives ¼ trust to each of the entities he knows, then 4 signatures on the public key of an entity You does not know would be required.

How many elements of trust which you can see from this diagram?



Exercise Question – E7.2(i)

Assuming that Alice has sent a signed message to Bob.

(i) Highlight the steps for verifying a digital certificate.

Exercise Question – E7.2(i) - A

- Check validity period to see if it is expired.
- Check CRL list to see if the certificate has been revoked.
- Verify the signature on the cert:
  - Calculate a message digest for the certificate
  - Use the CA's public key to decrypt the digital signature and recover what is claimed to be the original message digest embedded within the certificate
  - Compare the two resulting message digest values to ensure the integrity of the certificate

Exercise Question – E7.2(ii)

(ii) Highlight the steps Bob takes to verify the authenticity of the message from Alice.

Exercise Question – E7.2(ii) - A

- Verify the certificate or chain of certificates
- Verify Alice's signature