Exercise 1: In the public-key certificate system, suppose that the certificate authority (CA) employs DSS signature. Assume that CA's private key and public key pair is denoted by (sk_{CA}, pk_{CA}). Bob requests a public-key certificate for his key pair (sk_B, pk_B), which is a RSA key pair.

(a) Explain what Bob should submit to the CA to get the certificate for his public key pk_B.

Using the following information, the certificate authority will generate a digital signature to bind Bob's secret key with his public key:

- pk_B
- Bob's identity
- Expiration date
- Scope of key (encryption/signing)

(b) How does CA generate the certificate of Bob's public key? (You only need to specify the format of the certificate).

This procedure is performed by creating a digital signature using the certificate's own secret key. The format is as follows:

$$Certificate_{pk_B} = Signature_{CA}(pk_B, Bob's\ identity, Expiration\ Date, Scope\ (enc/sig))$$

(c) When Alice wishes to send some sensitive information to Bob using Bob's public key, what does she need to do before she performs the RSA encryption using Bob's public key?

Alice must verify Bob's identity first – in order to do so, she must verify the public key in her possession is Bob's, and not an adversary's public key. To verify Bob's identity, she must contact the CA, which will return a certificate generated using their own digital signature to bind Bob's identity and public key, as shown in part b). Alice is then able to decrypt the digital signature using the CA's public key to verify Bob's identity and public key. Once verified, Alice can encrypt her message using Bob's public key before sending it to him.

(d) Why is a certificate authority necessary for a public-key system?

A certificate authority converts a peer-to-peer trust assumption to a multiple-to-one trust assumption in the public key infrastructure. By assuming that the CA's public key is unique, every user must now trust that CA. Without a trusted CA, everyone is able to issue their own keys and this decreases the level of trust with respect to authentication. A trusted CA is the only entity that can issue trusted digital certificates, allowing trusted authentication between peers. [1]