X509 and PKI

1. What is the reason for having the X.509 standard?
2. What is the difference between PKI and PKIX?
3. Define each of the following terms in the context of PKIX:
    a. Initialization
    b. Registration
    c. Certification

    What are the security threats related to inappropriate execution of each of these functions?

4. What is the reason of having the third message in the three-way authentication exchange using X.509?
5. The three authentication exchanges of X.509 use timestamps AND nonces. Why?
6. The three-way exchange as described in X.509 is flowed if (as said in the standard) time stamps are not checked. Can you find how E can convince B that she is A under this exchange (if timestamps are not checked). Suggest a solution that does not involve using timestamps.
7. Which of the following is not a valid certification confirmation chain:
    a. A<<B>>B<<C>>C<<D>>D<<X>>
    b. A<<B>>B<<C>>D<<C>>D<<X>>
    c. A<<B>>C<<C>>C<<D>>D<<X>>
8. What is wrong (if any) if the authentication exchanges of X509 was changed as follows:
    a. ID_B was removed from message 1
    b. r_B was removed from message 2
    c. K_{ba} was removed from message 2
    d. t_B was removed from message 2
    e. ID_A was removed from message 2
    f. r_B was replaced with $H(r_B)$ in message 2
    g. r_B was replaced with r_B+1 in message 2
    h. r_B was replaced with $E(K_{ab}, r_B)$ in message 2
    i. r_B was replaced with $E(K_{ba}, r_B)$ in message 2