Names: PJ Sangvong , Luisa Escosteguy

Simple Communication Scenarios

1. We will ensure confidentiality using symmetric encryption:

First Alice and Bob have to agree on a secret key K - they use Diffie-Hellman to do so. As PITM is not possible in this scenario, we are confident that only Alice and Bob have the shared secret key. Once they agree on K, Alice can send Bob AES(K, M) and Bob can do AES_D(K, C) to read the message. Eve does not have K, so she would not be able to read the plaintext message.

2. We will use public key encryption with SHA-256 (provides data integrity check and the long message will be suitable to do public encryption) and a digital signature.

Alice computes Sig = E(S_A, H(M)), and sends M || Sig. Bob then checks if H(M_received) == E(P_A, Sig). If those are equal then Bob is sure that the message came from Alice and it is the original message. Otherwise, the message is corrupted by Mal. Here, Mal can read the message and modify it. However, if Mal modifies the message, Bob will be able to tell that it was corrupted when verifying the hash.

3. Symmetric encryption with signature using public encryption and hash:

First Alice and Bob have to agree on a secret key K - they use Diffie-Hellman to do so. As PITM is not possible in this scenario, we are confident that only Alice and Bob have the shared secret key. Once they agree on K, Alice computes Sig = E(S_A, H(M)) and sends Bob AES(K, M) || Sig. Bob then checks if H(AES_D(K, M_received)) == E(P_A, Sig). Here, Eve cannot read the message, as she does not have K to decrypt the message. Furthermore, Bob will be confident the message came from Alice because she is the only one that has S_A.

Questions about breaking security

4. Alice can claim the following happened:
    1. Alice wrote her private key on a paper and lost it, and someone found it and used it to fake her Sig_A and send the altered contract to Bob.
       Plausibility: A judge would not believe Alice physically lost the key. It doesn't make sense to write the key on a paper and just lose it in a public place (at least we hope). Furthermore, the chances of someone finding the paper before it degrades and figuring out that it is a private key and using it to fake a contract are incredibly low.
    2. That P_A is not Alice's public key

    Plausibility: In real life, that is very unlikely, as we have the certificate authority as a trusted third party to make sure the public keys are legit.

   3. There was a person in the middle attack that had been spying on their communication channel from the beginning, and the person modified the contract when Alice sent Bob her contract.
      Plausibility: This is most likely the most plausible reason. Scenario 3 is not resistant to a person in the middle attack.

5. Sig_CA = E(S_CA, H("bob.com" || P_B))

6. No, it is not enough, Cert_B is public and Eve could have forwarded it, faking to be Bob. Alice has to verify that Bob has a secret key by sending something to Bob that is encrypted with P_B and have Bob send that back to see if he is able to decrypt it or not. If he can, then he has S_B.

   One way to do this is for Alice to send Bob her public key encrypted with Bob's P_B (E(P_B, P_A)) and a random number also encrypted with P_B. Then, Alice will tell Bob to decrypt the message with his secret and use the P_A to send the encrypted message of the random number back. If Bob is able to decrypt her message, he will have P_A and the random number that Alice comes up with. Bob will then be able to encrypt the number with P_A and send it back to Alice as a verification that he has S_B.

7. The certificate-based trust system could be undermined as follows:
   1. Mal can buy a certificate claiming she is Bob. She can do that by providing all the verification needed to the CA - if Mal has the correct documentation and addresses, the CA will genuinely believe Mal is Bob, and therefore Mal has Bob's identity.
   2. Mal can break into Bob's place to steal their secret keys. If Mal has Bob's secret and public key (publicly available), then she can claim she is him.