Scenarios

Author: Lily Li
Conferred with: Jeff Ondich

1:

Plan:
Alice and Bob use Diffie-Hellman to agree on a shared secret key K.
Then they can use the symmetric encryption algorithm AES and the Key K to send encrypted messages to each other, AES(K, M), and decrypt using the same key.

Explanation:
Given PITM is impossible, Alice and Bob would be able to agree on a key K securely with Diffie-Hellman.
The AES algorithm is fast and efficient for long messages, and without the key K, Eve wouldn't be able to decrypt M.

2:

Plan:
Alice could prevent message altering by using Data Signatures.
She could send Bob, the concatenation of her message, with a digital signature (the hashed digest of the message (using SHA-256) encrypted with Alice's private key)
This is what Alice will send:

$M \,||\, Sig_A$

$Sig_A = E(S_A, H(M))$

Explanation:
Given that only Alice has the Secret Key S_A, Eve would not be able to reconstruct the digital signature. Therefore, if she attempts to alter the message, changing M to M', Bob will notice after he decrypts Sig_A with P_A that H(M') is not equal to H(M).

3:

Plan:
Alice and Bob use Diffie-Hellman to agree on a shared secret key K.
Combining AES encryption and Digital Signature, Alice sends Bob:

C_A = AES(K, (M || Sig_A))
Sig_A = E(S_A, H(M))

This way, Eve wouldn't be able to read the message, and Bob can verify the message with Alice's signature.

Explanation:
Since PITM is impossible, Alice and Bob would be able to agree on a key K securely with Diffie-Hellman, and exchange long encrypted messages using AES efficiently.
Given that only Alice has the private key, only she would be able to construct the signature.
When Bob decrypts the message with K, he could hash the message and compare it to that of in the signature to be sure that this is the message Alice sent as in the following:

AES_D(K, C_A) = M || Sig_A

H(M) = D

E(P_A,Sig_A) = D'

If D == D', Bob knows all is good.

4:

A) Alice: Bob figured out Alice's private key through her public key and created (C || Sig) by himself.

Plausibility:
Not very plausible, this claim means that Bob broke RSA, factored an extremely large prime…unless he was crazy lucky, it would take till the end of the universe to do it brute force.

B) Alice: Eve intercepted an erroneous version of the contract and sent it to Bob as a final version, claiming that she is Alice.

Plausibility:
This is plausible. With the PITM attack, Eve could have obtained the AES key K and decrypt the communications between Bob and Alice and send intercepted packages to any party.

C) Alice: Eve stole Alice's private key and constructed a mal-intentioned contract, to send to Bob.

Plausibility:
This is plausible, but needs to be considered with the specific security measures Alice was using to safeguard her private key. However, if Eve manages to obtain Alice's private key, she would be able to construct such a contract, sign it as Alice, and send it to Bob.

5:

Sig_{CA} is a hashed version of validated data (the domain name, and its affiliated public key, and other data…) Encrypted with CA's private key. Therefore, everyone with CA's public key will be able to validate such data, but no other people can construct such a signature.

$Sig_{CA} = E(S_{CA}, H("bob.com" || P_B))$

6:

No, anyone may have intercepted Bob's certificate and sent it out.
To validate that it is Bob who is speaking, Alice could send Bob some random message encrypted in Bob's public key, requiring Bob to send back the original random message. Only Bob with it's private key will be able to decrypt it and send it back.

7:

A) Someone physically breaks into CA, and gain access to their secret key and can sign everyone
B) Eve convinced CA that Eve owns a domain that it doesn't own and CA gives Eve a certificate
C) Eve steals certificates that doesn't belong to her