5.3 Question 3

5.3.A Is scenario 2 safe against man-in-the-middleattacks? Why?

No, it is not, as a malicious entity/adversary E can intercept the messages sent between A and B. A following scenario can be used as an example for such an attack:

1. A generates public/private key pair $\{PU_a, PR_a\}$ and sends $PU_a \| ID_A$ to B
2. E intercepts message, creates its own public/private key pair $\{PU_c, PR_c\}$ and sends $PU_c \| ID_A$ to B
3. B thinks the message comes from A and performs the encryption using a generated secret key K_s and sends $E(PU_c, K_s)$ to A
4. E intercepts message decrypts message from B, learning K_s
5. E sends $E(PU_a, K_s)$ to A

As E knows K_s the adversary can eavesdrop the messages sent between A and B and is able to decrypt the messages using K_s.

5.3.B In scenario 1, is each side confident about the authenticity of the other side? Why?

As in step 2 the nonce $N1$ is being send concatenated with nonce $N2$ it ensures A that this message comes from B as only B is able to decrypt $N1$ from the first message. As in step3 A uses the public key of B to encrypt $N2$, B can be assure that it is communicating with A. Then A sends the message $E(PU_b, E(PR_a, K_s))$ to B which is ensuring that only B can read it as it is encrypted using B's public key and that this message comes from A as K_s is encrypted using A's private key. Hence, this scenario ensure confidentiality and authenticity.

5.3.C In scenario 1, assume that in step 2 only nonce 2 is being transmitted (and not nonce 1). In the end of step 4, which side is ensured about the identity of the other side? Why?

As written before $N1$ is being sent to A to ensure that the Responder B is actually the "wanted" responder. Therefore, in the end only B can be assure that it was talking with the "wanted" Initiator A.