Phi Rapacz

1) An AES exchange between Alice and Bob, using a secret key chosen via DH should suffice. Because the M is long, it is most reasonable to break it up into blocks. Because we are not concerned with AITM, DH protects from evesdroppers well.
2) Once a DH key exchange has occurred, Alice should send a random number R to Bob, and demand $E(S_B, R \,||\, g^b \bmod p)$. If $E\_D(S_B, R \,||\, g^b \bmod p)$, if $g^b \bmod p$ isn't what Alice expected it to be, then she knows that there was someone without Bob's secret key in the middle of their exchange: only bob could have encrypted with his secret key (given out assumptions), so if the DH "half" is different from what Alice expected, there was an AITM who created their own DH keys with both Alice and Bob.
3) After agreeing on a key K via DH, Alice can use S_A and then AES to encrypt the message in blocks, so that Bob knows it was sent by Alice if $D(P_A, (AES\_D(C))$ works.
4) Alice can claim that an AITM changed the contract, which a knowledgeable judge would find suspect considering the difficulty of changing a signature to match the changed message. Alice could claim that she never had any exchange with Bob, but given the assumption that all parties have kept their private keys truly private that also seems unlikely (only Alice could have encrypted anything decryptable with her public key). Alice could claim that Bob changed the contract after the fact, but this is again undercut by the fact that Bob assumedly does not have Alice's secret key, and could therefore not re-encrypt an edited contract and corresponding hash digest signature.
5) $E(S_{CA}, H(\text{"bob.com"} \,||\, P_b))$
6) Bob could encrypt a challenge number R from Alice, $E(S_B, R)$. This should be decryptable by P_B if it is truly Bob.
7) If Mal owns both "Bob" and the CA, this is wildly untrustworthy - the third party is no longer a third party; if Mal manages to convince the CA that they are bob.com, (if Bob has perhaps not registered with the CA or Mal claims "their" previous key pair is compromised and needs to re-register) the public key now affiliated with Bob is instead Mal's.