Author: Tianyi Lu

Scenario 1

If AITM is impossible, Alice and Bob and directly use Diffie-Hellman key exchange to agree on a shared secret key K, then they can use AES encryption with their secret key K to encrypt their long messages. In this way, Eve can only observe the ciphertext $C = \mathrm{AES}(K, M)$ and has no way to read the plaintext M.

Scenario 2

We can construct a digital signature using Alice private key and concatenate is with the long message. The entire content will be $M \mid\mid \mathrm{E}(S_A, H(M))$. Upon receiving the content, Bob can use Alice's public key to decrypt the hash of the message as

$$H(M) = \mathrm{E}(P_A, \mathrm{E}(S_A, H(M)))$$

Then, Bob can calculate the hash of the actual message himself and compare the two hashes. If they're equal, the message is intact. If not, the message is modified. Mel cannot temper with the signature because he doesn't have Alice private key and therefore cannot encrypt the signature correctly.

Scenario 3

Since it's impossible to do AITM, Alice and Bob can still use Diffie-Hellman key exchange to agree on a shared secret key K. However, to make sure Alice is sending the message, Bob can pose a challenge to Alice. Bob will generate a random number R while Alice has to response with $E(S_A, R \mid\mid g^a \bmod p)$ where $g^a \bmod p$ is the public component for Alice's key exchange. Since Bob has the correct public key for Alice, Bob can decrypt this encryption to confirm the correctness of the incoming R and $g^a \bmod p$. If all checks out, Bob is now sure he had a key exchange with the real Alice. For now on, Alice can use $AES(K, M)$ to send encrypted long message to Bob without exposing the plaintext to Eve.

Scenario 4

In this scenario, there are a few potential explanations Alice could present.

Somebody Forged the Contract:

Claim

Alice could claim that the contract C is forged, and then generated the digital signature Sig using Alice's private key, which someone somehow got unauthorized access to.

Plausibility

If Alice's private key is proven to be compromised (which is a big "if"), this scenario is plausible. However, it would raise serious questions, such as how someone could gain access to her private key. If Alice kept her private key secure and there's no evidence of any compromise, then this claim becomes less believable.

AITM Attack

Claim

Alice might argue that when she sent the original contract to Bob, Mal intercepted the document in transit, altered it, and then sent the altered version to Bob. This would mean the contract Bob received (and subsequently signed) wasn't the original she sent.

Plausibility

While AITM attacks are theoretically possible, in this case, the digital signature would not verify against the tampered document using Alice's public key unless Mal also had access to Alice's private key. Therefore, without evidence of private key compromise, this claim also becomes less convincing.

Alice Signed a Different Contract:

Claim

Alice could suggest that she signed a different contract and that Bob presented a completely different contract to the court. She might claim the signed contract she has on her end differs from what Bob has produced.

Plausibility

The claim can be verified by checking the hash of C in the signature. We can first calculate the hash value of the document provided by Bob and compare that to the hash value in the signature decrypted using Alice's public key. If they are the same, then Alice's claim is false.

Scenario 5

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

Scenario 6

No, because $Cert_B$ is a public information. Mal can acquire Bob's certificate and send it to Alice.
To be sure that Alice is talking to Bob, Alice can pose a challenge to Bob. Bob need to send Alice $E(S_B, H(P_B))$. After receiving the message, Alice can decrypt it using P_B, calculate and compare the hash value of P_B in the certificate with the hash value of P_B from the challenge. If they are the same, Alice can be certain Bob has S_B.

Scenario 7

Compromised CA

If the CA itself is compromised, malicious actors could issue certificates in any name they choose, including Bob's. This is one of the most damaging attacks since it undermines the trust in every certificate issued by that CA.

Stolen Private Key

If Bob's private key is stolen or leaked, Mal could use it to impersonate Bob. Mal could present Bob's certificate (which is public) and use the stolen private key to sign any messages or establish secure connections.