Almost there …

✓ Does ensure the confidentiality of the communication

✓ Does authenticate Alice and bob

✓ Does prevent replay attacks

➡ But how to ensure the authenticity of the public keys without using a Public Key Server ?

Trust Models