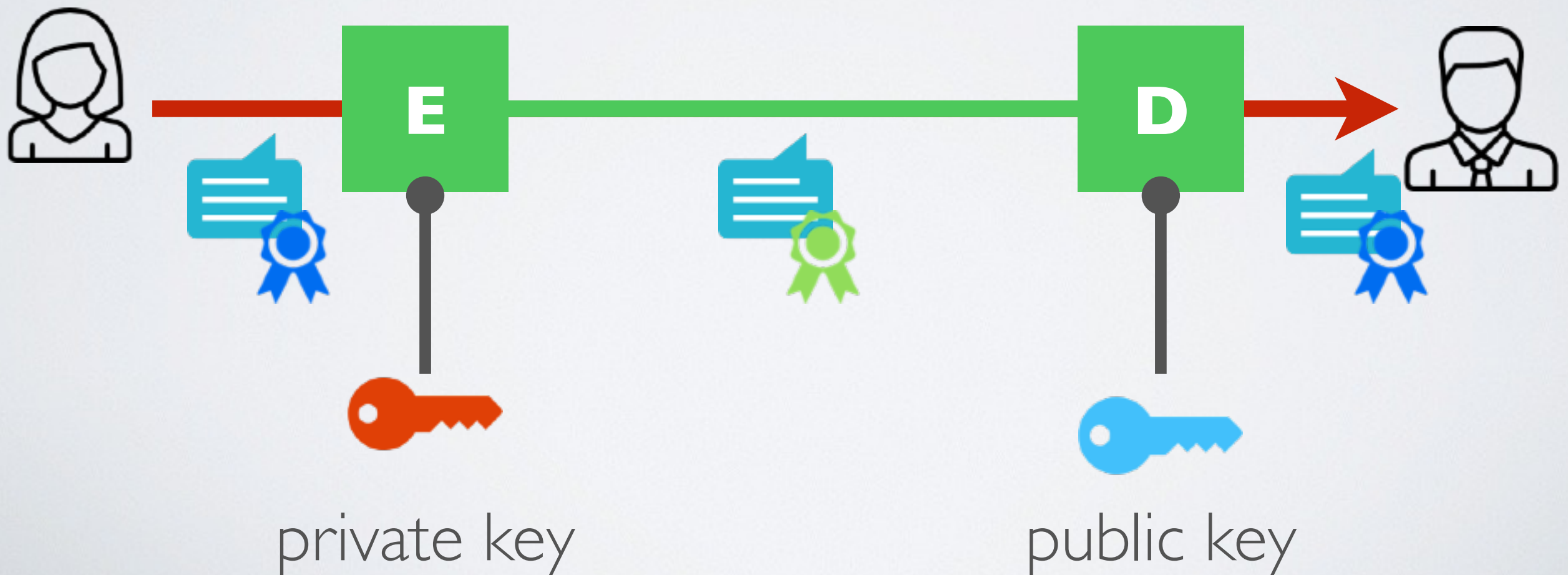
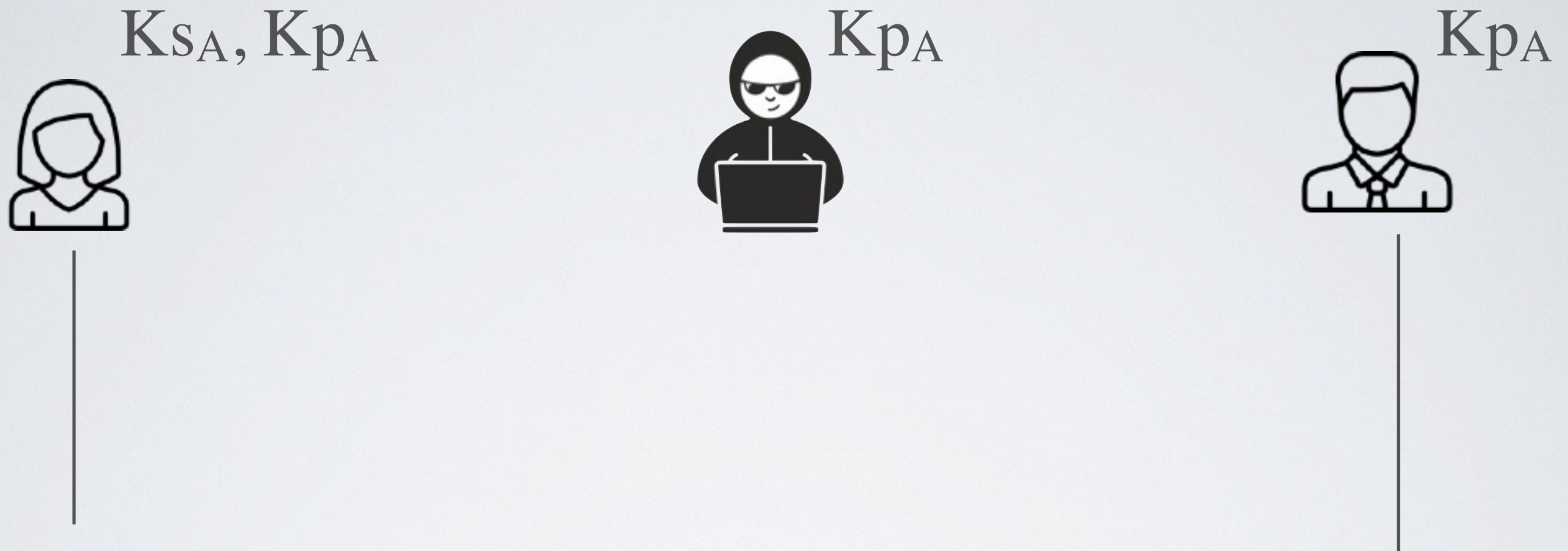


Asymmetric encryption: Digital Signature

- ➔ The private key for encryption
- ➔ The public key for decryption



Asymmetric encryption for **integrity**



Alice encrypts a message m with her private key K_{SA}

➔ Everybody can decrypt m using Alice's public key K_{PA}

✓ Authentication with non-repudiation (a.k.a Digital Signature)