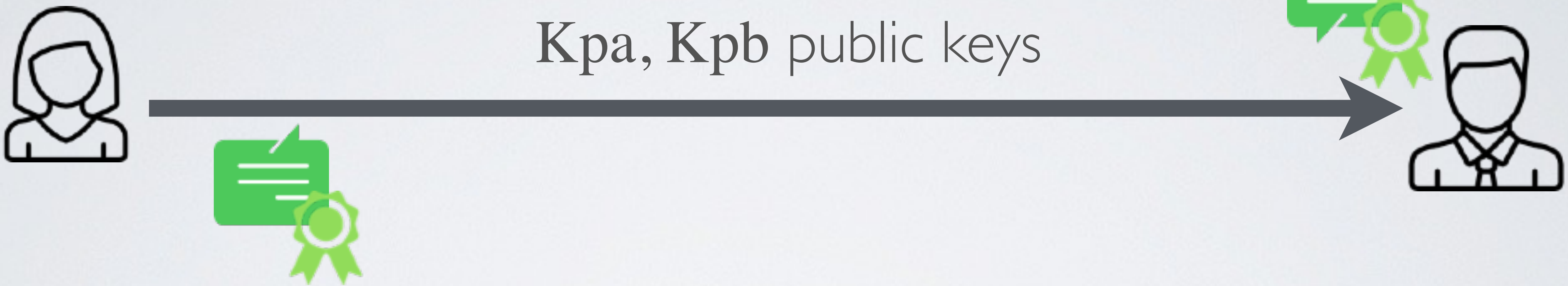
Digital Signature



Ksa Alice's Secret Key

Kpa, Kpb public keys

Ksb

- ➡ Use public cryptography to **sign and verify**

$$m \,\|\, SIG_{Ksa}(m)$$

$$SIG_{Ksa}(m) = E_{Ksa}(H(m))$$

Non-repudiation as a special case of integrity

	MAC	Digital Signature
Integrity	✓	✓
Non-repudiation	✗	✓