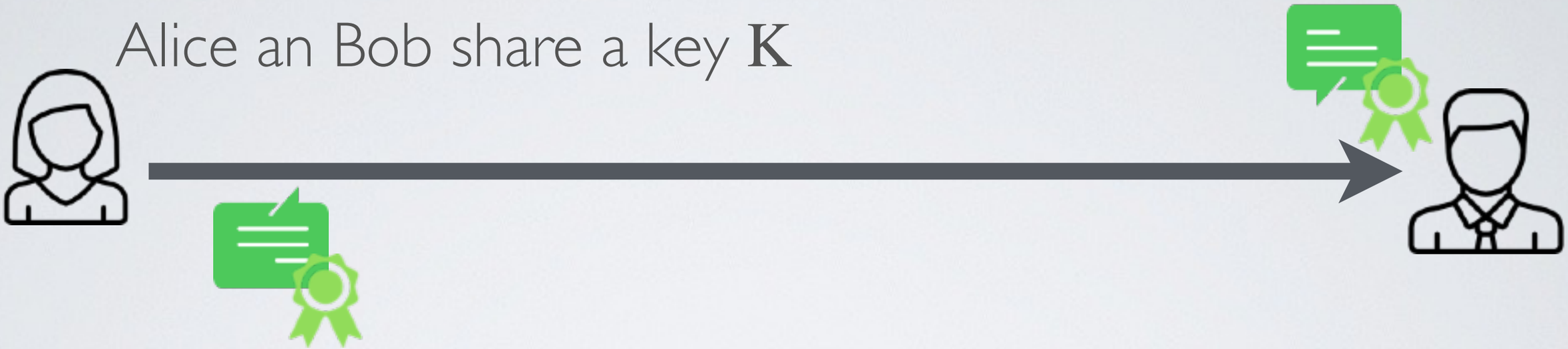
Security mechanisms

	Encryption	MAC	Authenticated Encryption
Confidentiality	✓	✗	✓
Integrity	✗	✓	✓

Authenticated Encryption (2013)

Alice an Bob share a key $\mathbf{K}$



Encrypt-and-MAC (E&M)	$AE_k(m) = E_K(m) \mid\mid H_K(m)$	*SSH*
MAC-then-Encrypt (MtE)	$AE_k(m) = E_K(m \mid\mid H_K(m))$	*SSL*
Encrypt-then-MAC (EtM)	$AE_k(m) = E_K(m) \mid\mid H_K(E_K(m))$	*AES-GCM*