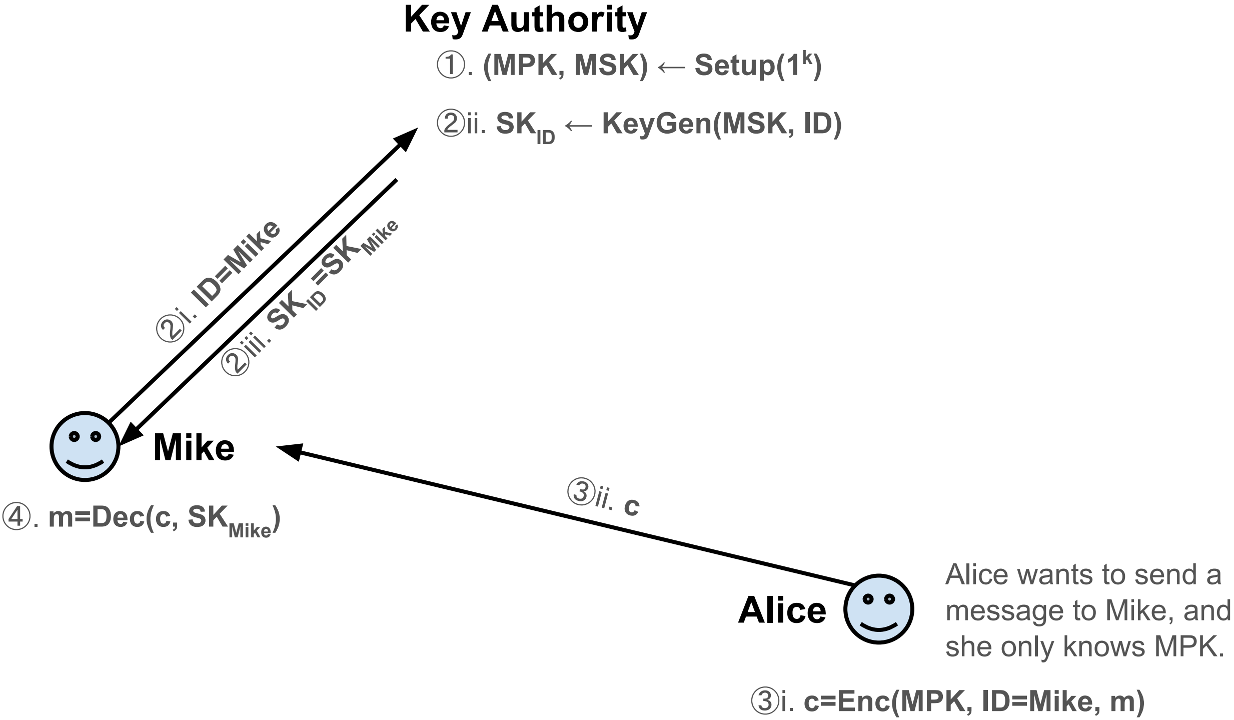

Key Authority

①. **(MPK, MSK) ← Setup(1^k)**

②ii. **SK_{ID} ← KeyGen(MSK, ID)**

②i. **ID=Mike**

②iii. **SK_{ID}=SK_{Mike}**

Mike

④. **m=Dec(c, SK_{Mike})**

③*ii.* **c**

Alice

Alice wants to send a message to Mike, and she only knows MPK.

③i. **c=Enc(MPK, ID=Mike, m)**