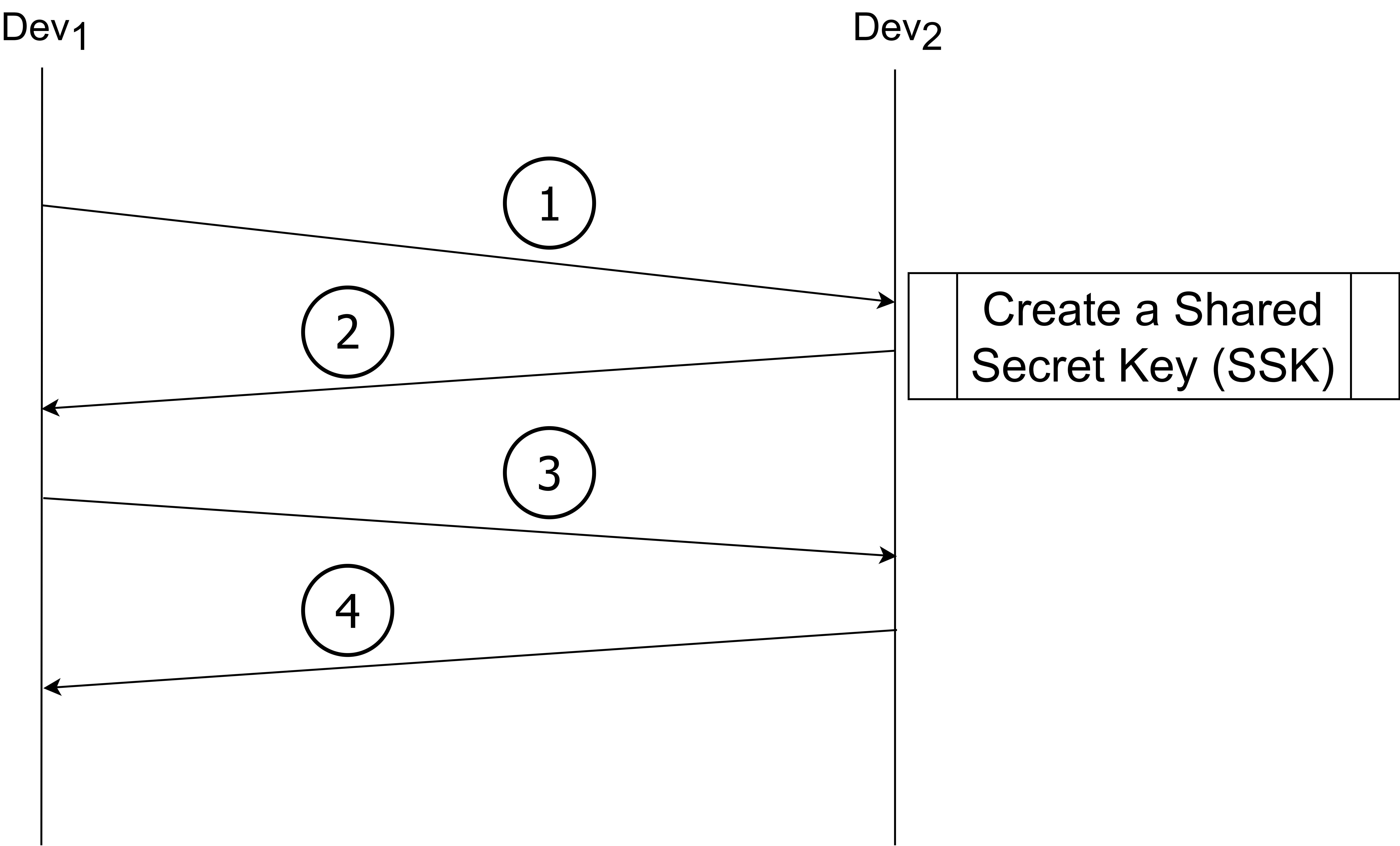


Protocol Description
1) ping, PK ₁ , Dev ₁ , sign _{PR1} (ping, PK ₁ , Dev ₁)
2) E _{PK1} (pong, PK ₂ , Dev ₂ , SSK, sign _{PR2} (pong, PK ₂ , Dev ₂ , SSK))
3) E _{SSK} (SND_msg1, sign _{PR1} (SND_msg1))
4) E _{SSK} (SND_msg2, sign _{PR2} (SND_msg2))



Dev₂: Device 2

PK₂: Dev₂'s public key

sign_{PR2}(...): signing with Dev₂'s private key

E_{PK1}(...): encryption with Dev₁'s public key

SND_msg2: custom message sent by Dev₂

Dev₁: Device 1

PK₁: Dev₁'s public key

PR₁: Dev₁'s private key

sign_{PR1}(...): signing with Dev₁'s private key

E_{SSK}(...): encryption with SSK

SND_msg1: custom message sent by Dev₁