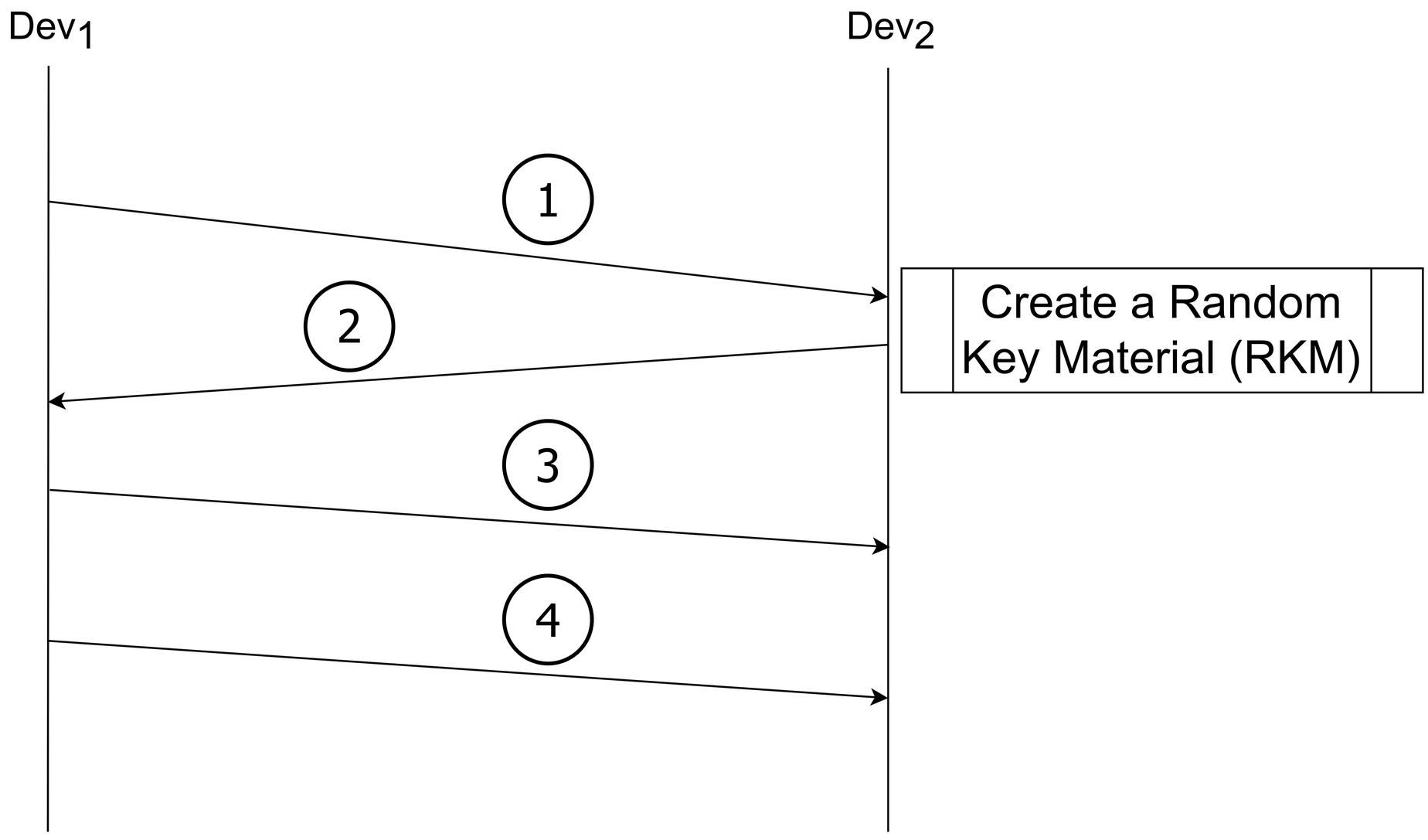
| Protocol Description |
| --- |
| 1) $Dev_1$, $Dev_2$, $N_1$, $PK_1$ |
| 2) $Dev_1$, $Dev_2$, $N_2$, $E_{PK1}(RKM)$, $sign_{PR2}$("ping", $Dev_1$, $Dev_2$, $N_1$, $N_2$, $E_{PK1}(RKM)$), $MAC_{SSK}$($Dev_1$, $Dev_2$, "ReceiverDone") |
| 3) $Dev_1$, $Dev_2$, $MAC_{SSK}$($Dev_1$, $Dev_2$, "TransmitterDone") |
| 4) $E_{SSK}$(SND_msg1, $sign_{PR1}$(SND_msg1)) |
| SSK = h($N_1$, $N_2$, RKM) |




$Dev_2$: Device 2
$N_1$: Nonce created by $Dev_1$
$sign_{PR2}$(...): Signing with $Dev_2$'s private key
$E_{PK1}$(...): Encryption with $Dev_1$'s public key
$MAC_{SK}$(...): MAC with the secret key
SND_msg2: Custom message sent by $Dev_2$
h(...): hash function (SHA-256)

$Dev_1$: Device 1
$PK_1$: $Dev_1$'s public key
$PR_1$: $Dev_1$'s private key
$sign_{PR1}$(...): Signing with $Dev_1$'s private key
$E_{SSK}$(...): Encryption with SSK
SND_msg1: Custom message sent by $Dev_1$