PERC Architecture Overview

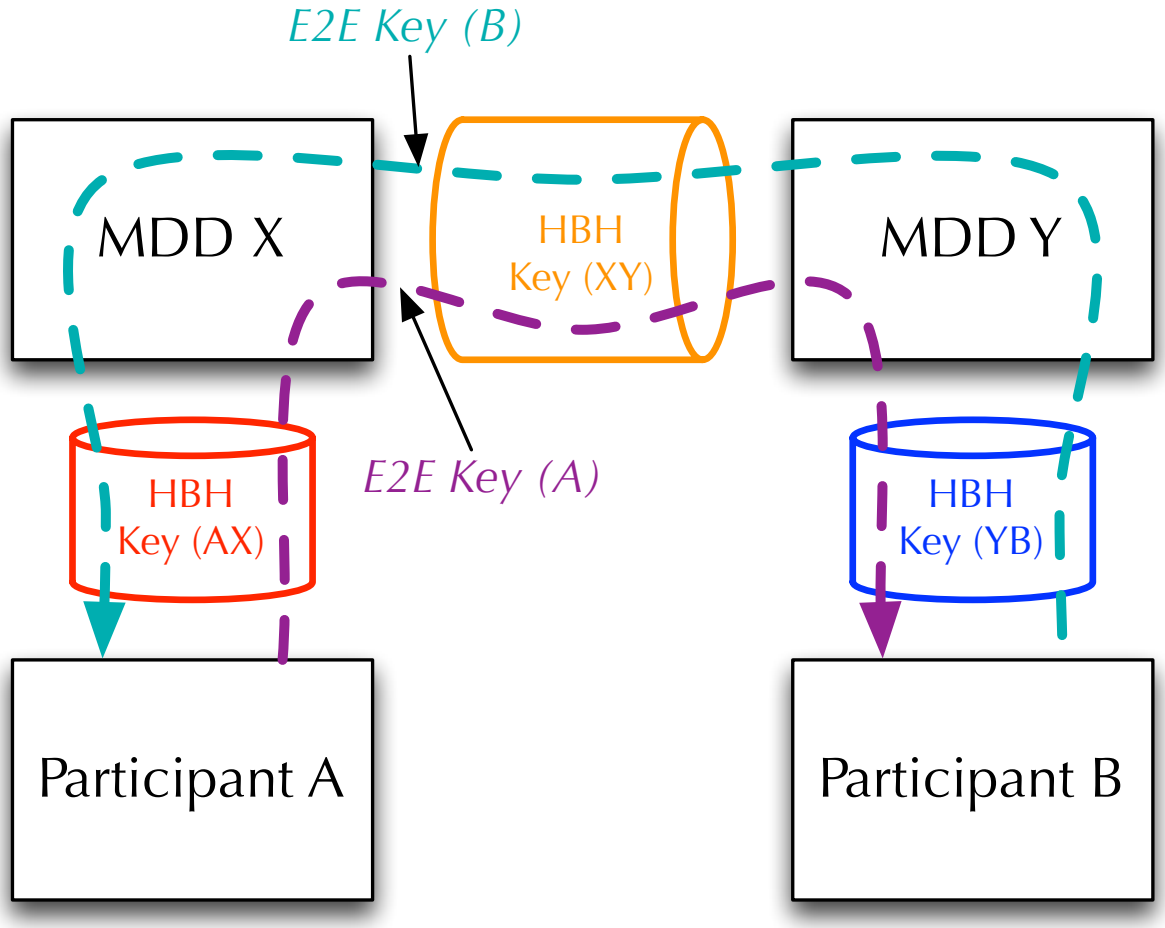
Adam Roach <adam@nostrum.com>

April 4, 2016

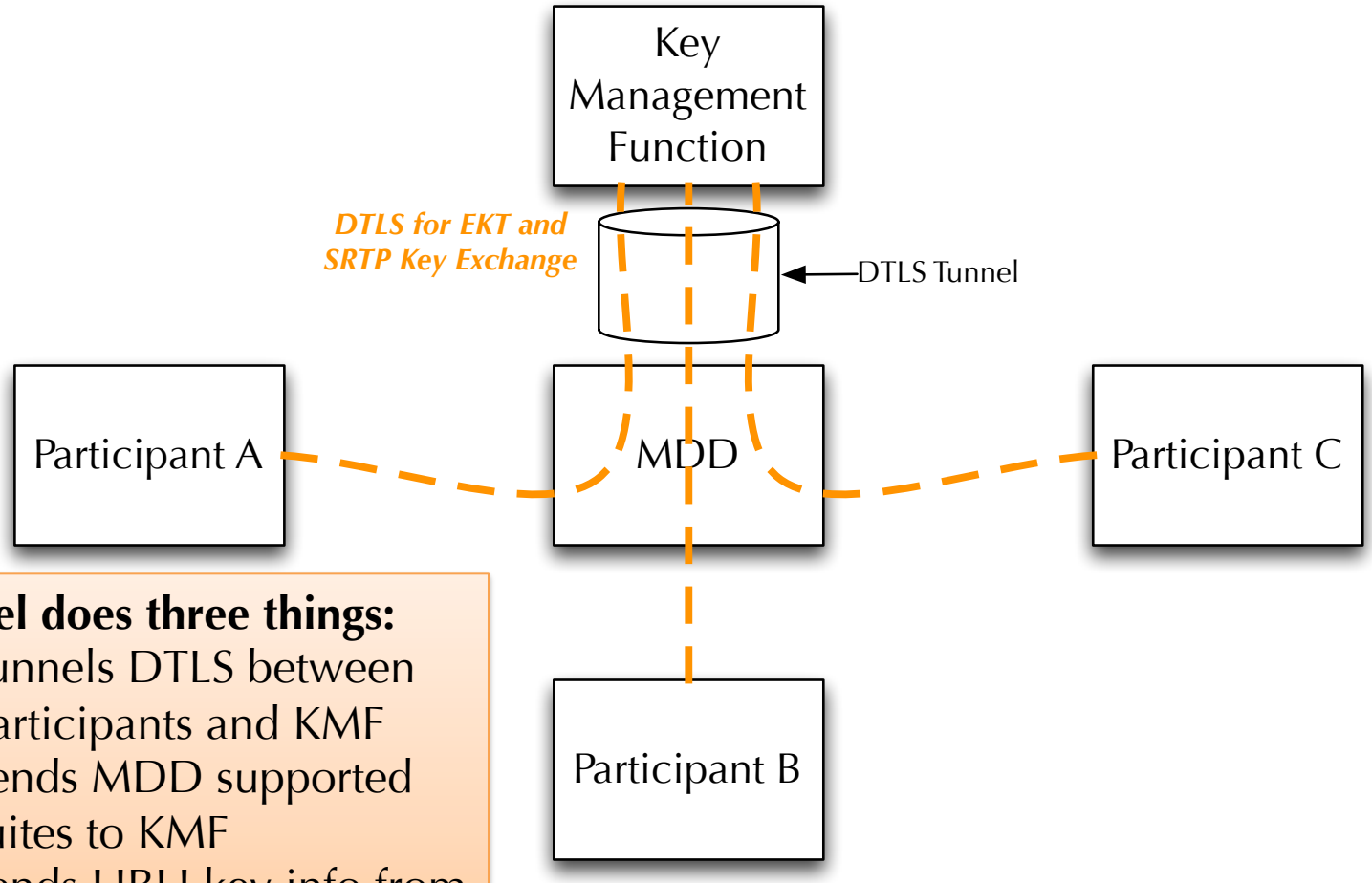
Relevant Drafts

- draft-jones-perc-private-media-framework
- draft-jennings-perc-double
- draft-jennings-perc-srtp-ekt-diet
- draft-jones-perc-dtls-tunnel

"Outer" (HBH) Keys and "Inner" (E2E) Keys (multiple MDDs)



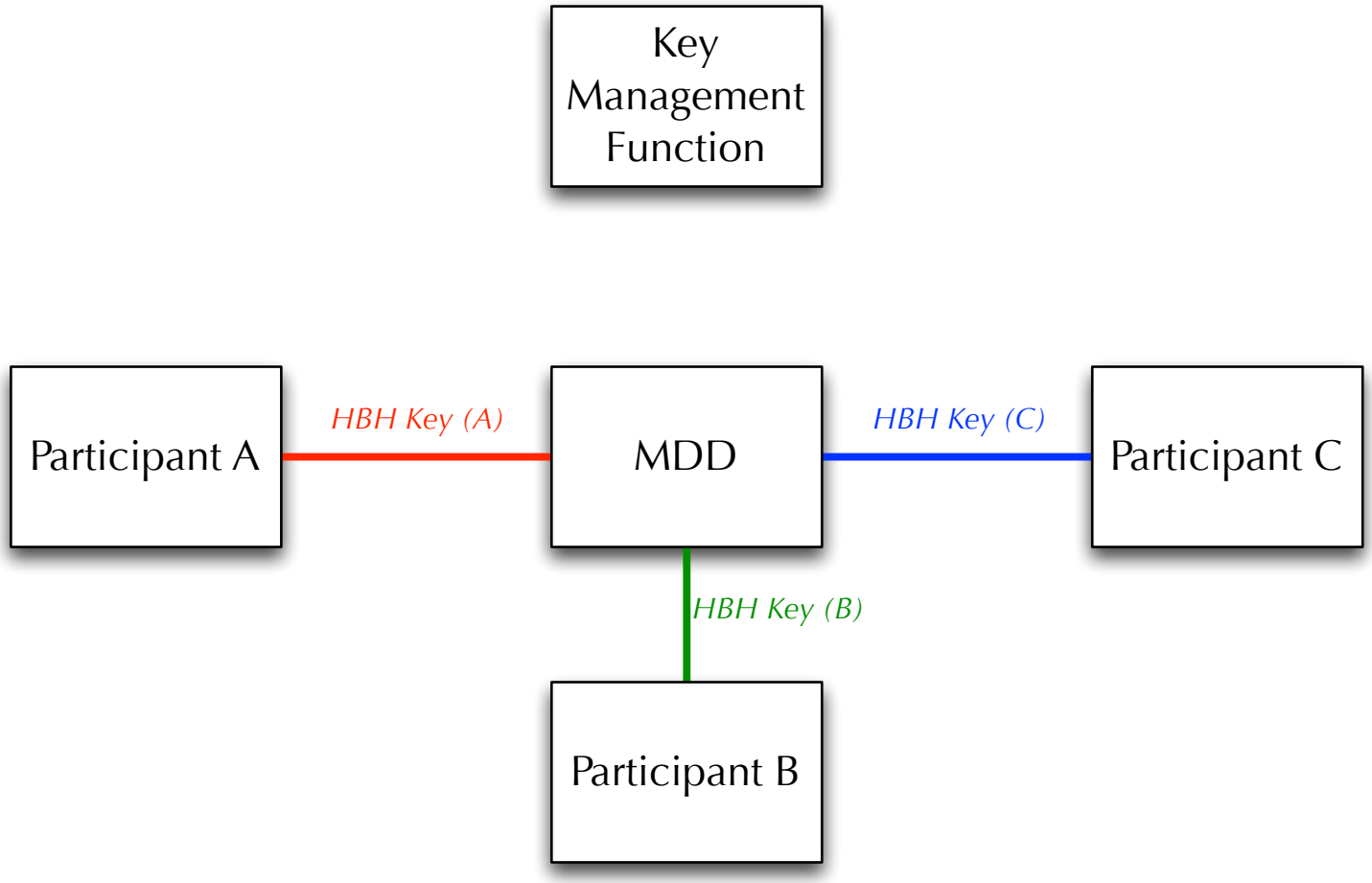
DTLS for Key Management



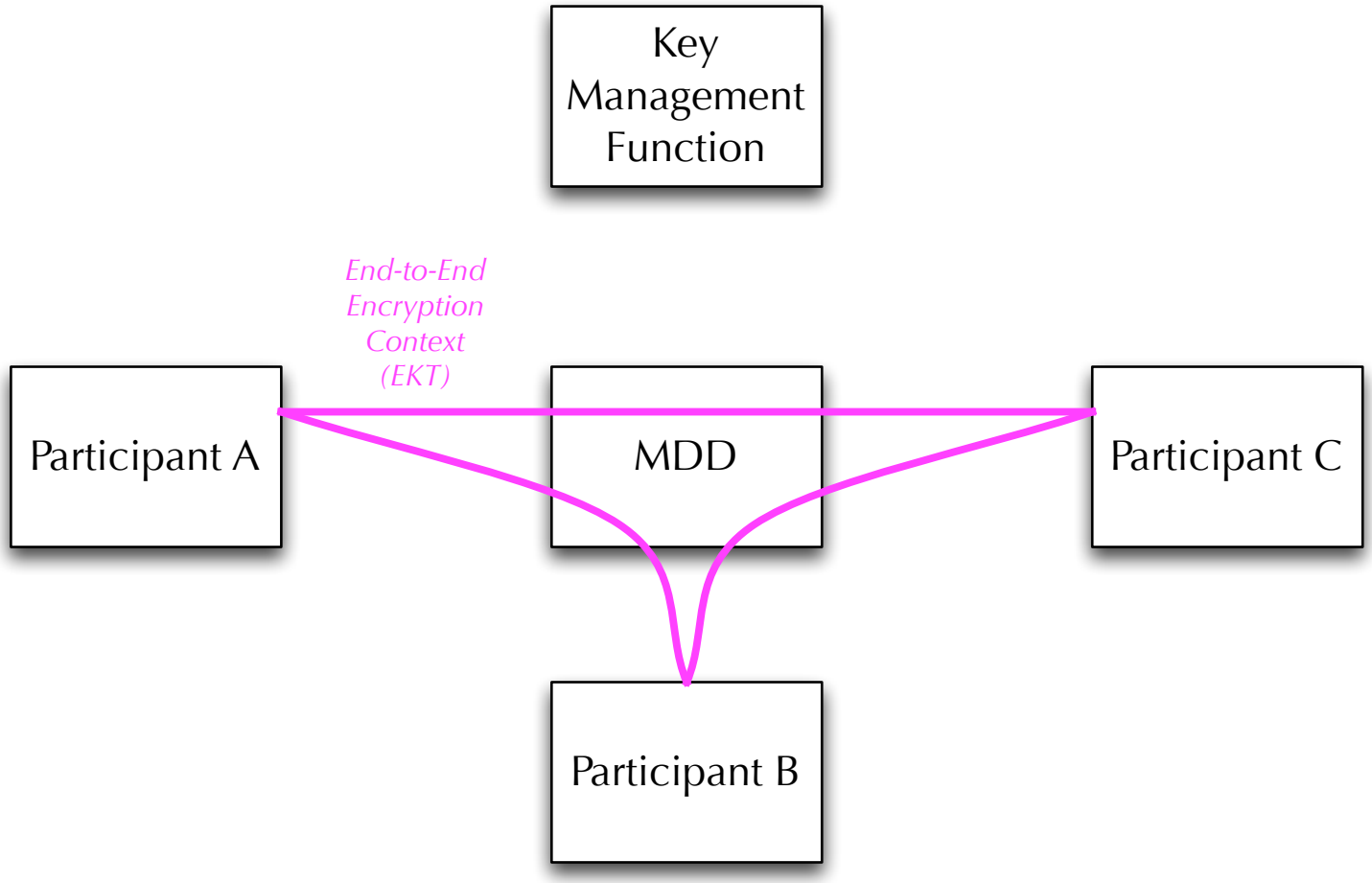
Tunnel does three things:

1. Tunnels DTLS between participants and KMF
2. Sends MDD supported suites to KMF
3. Sends HBH key info from KMF to MDD

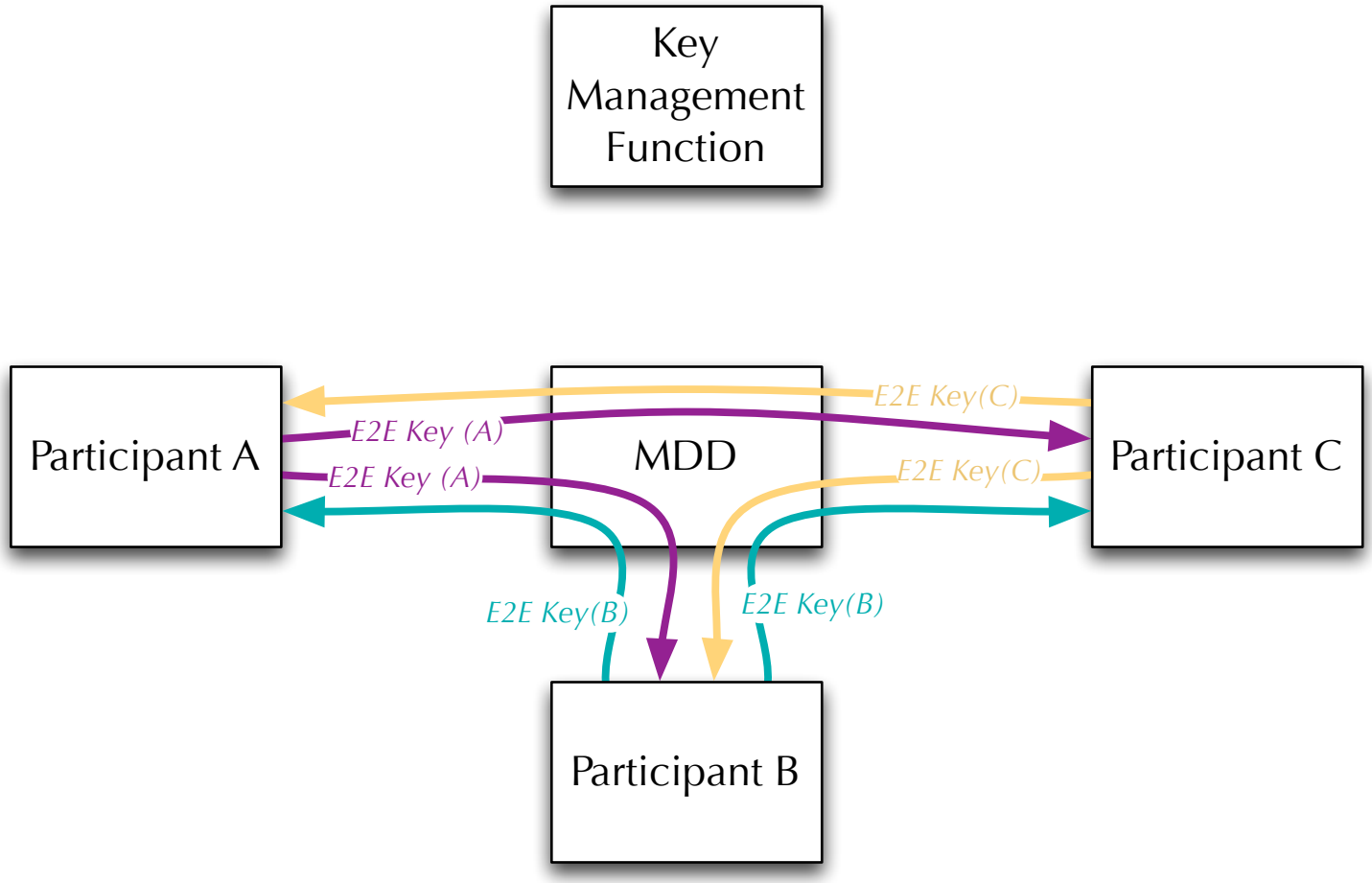
Hop-by-Hop Keys



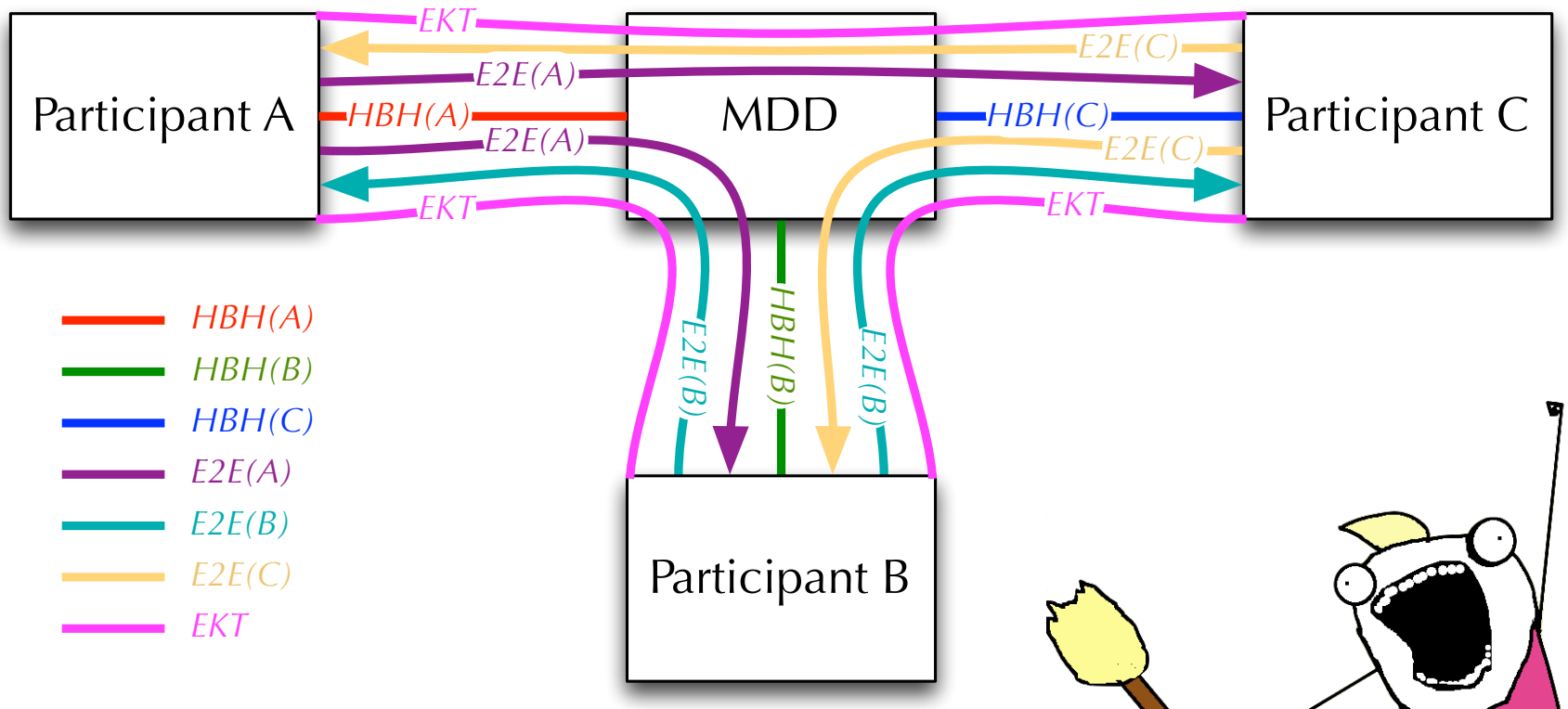
Shared Encryption Context (EKT)



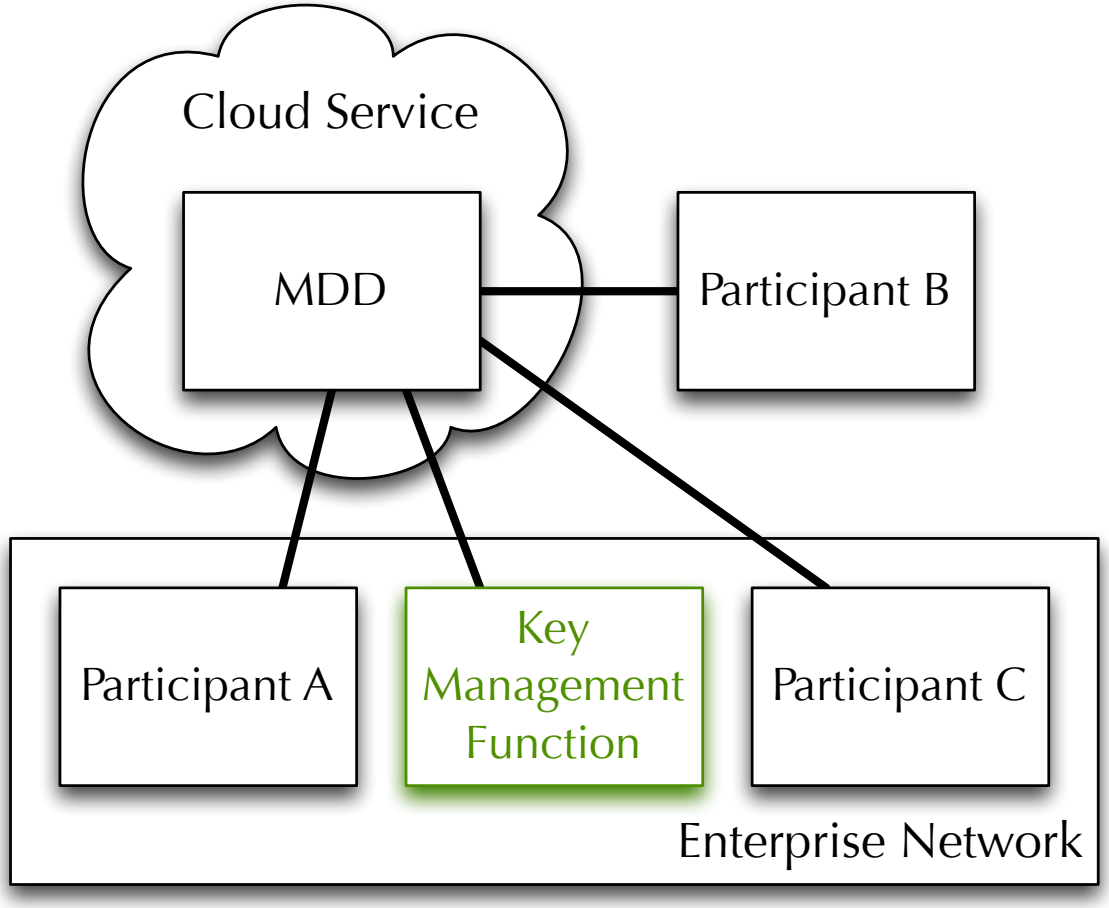
E2E Keys


Key Management Function
Participant A
MDD
Participant C
Participant B
E2E Key (A)
E2E Key (A)
E2E Key(C)
E2E Key(C)
E2E Key(B)
E2E Key(B)

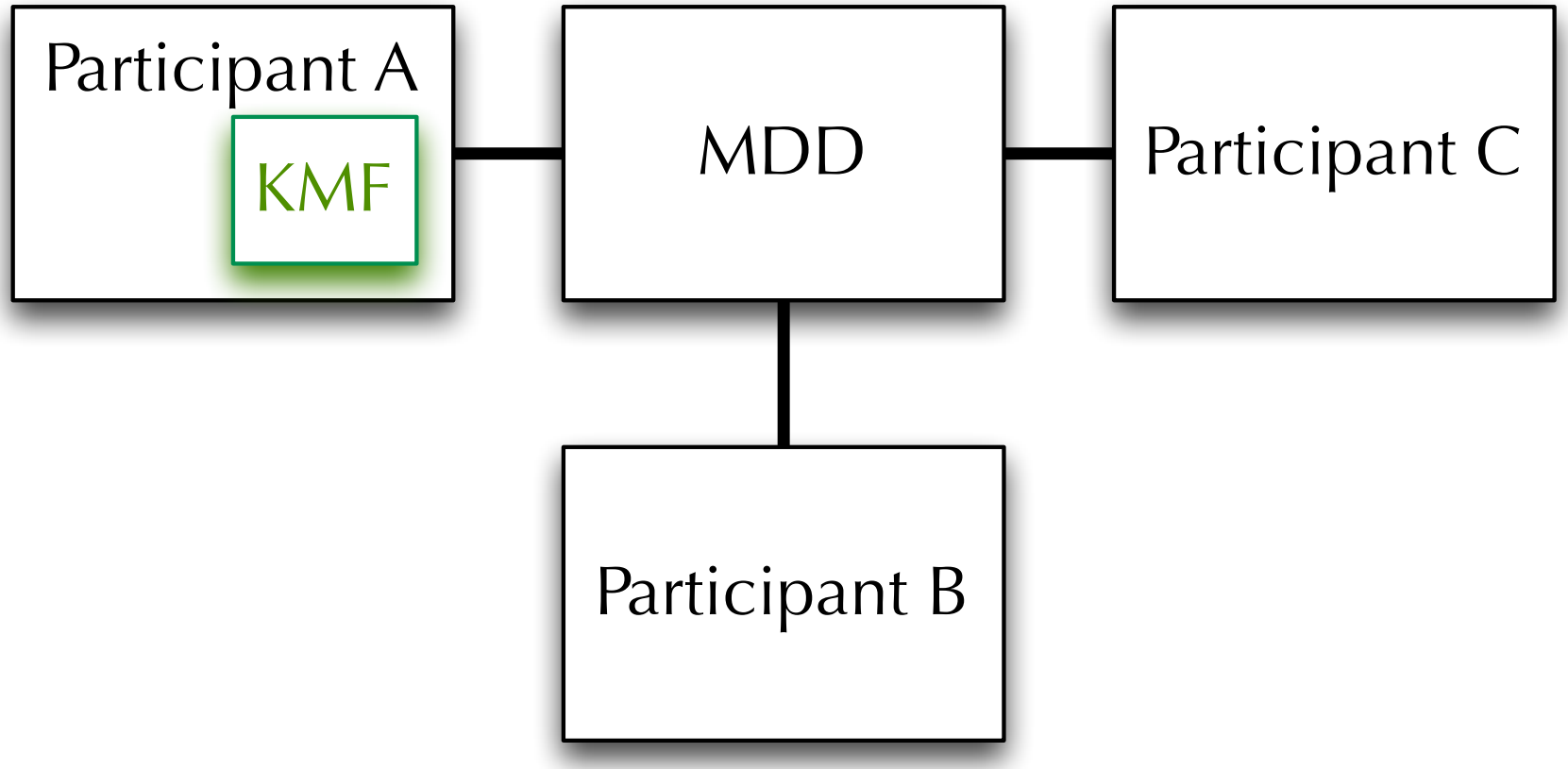
All The Keys!


Participant A
MDD
Participant C
Participant B
EKT
E2E(A)
HBH(A)
E2E(A)
EKT
E2E(C)
HBH(C)
E2E(C)
EKT
E2E(B)
HBH(B)
E2E(B)
HBH(A)
HBH(B)
HBH(C)
E2E(A)
E2E(B)
E2E(C)
EKT

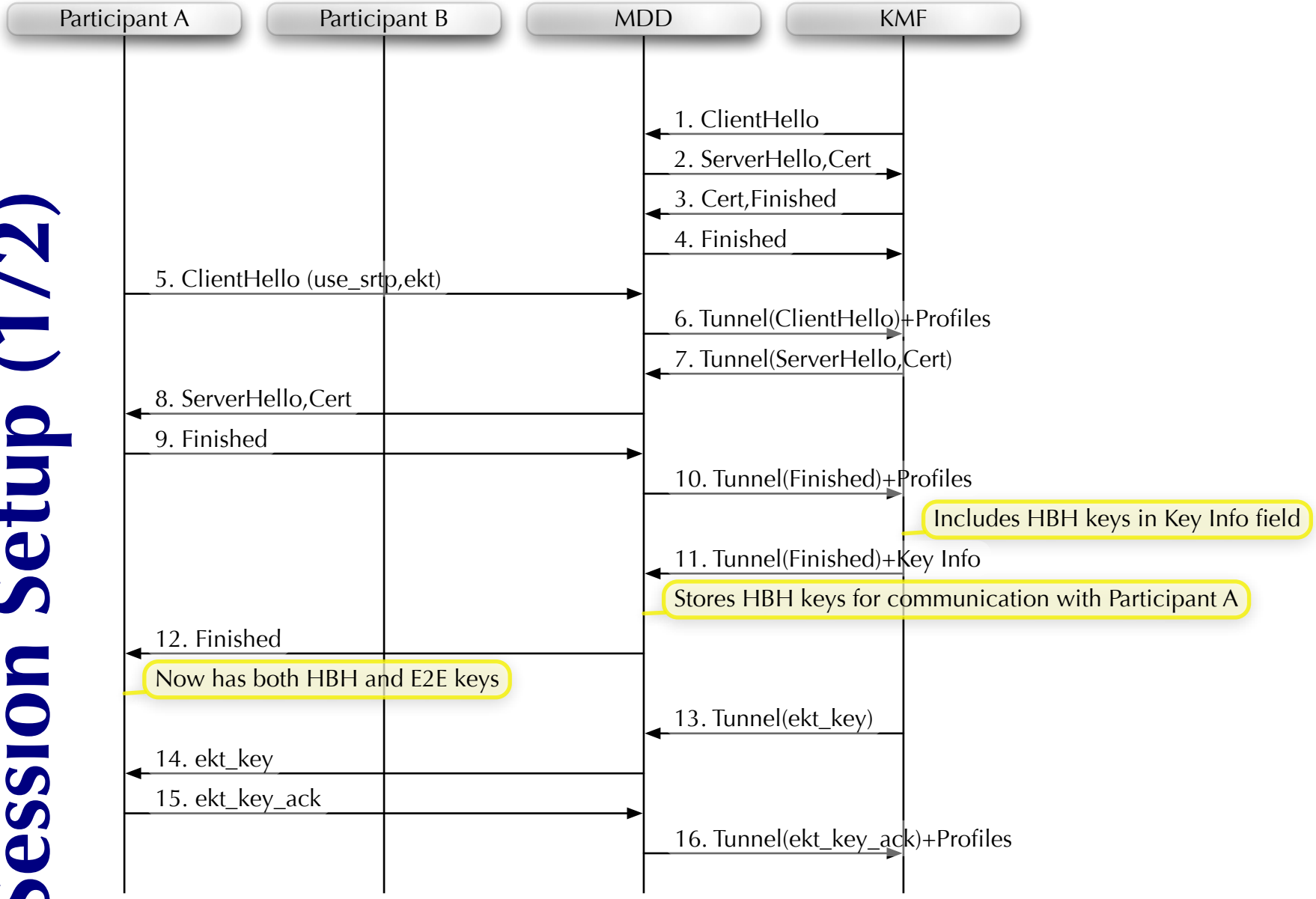
Example Deployment: Enterprise Cloud Services



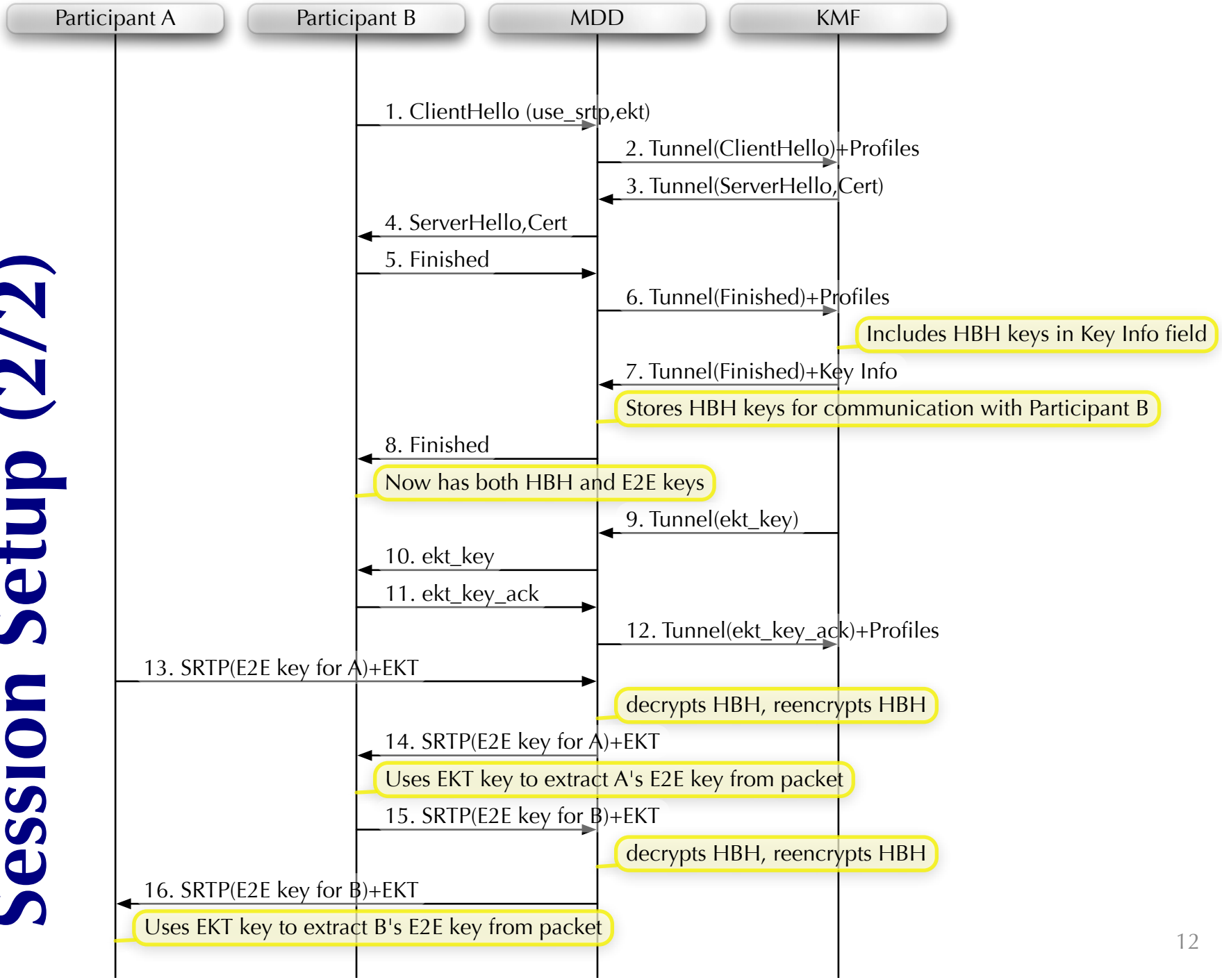
Example Deployment: Public Internet Service



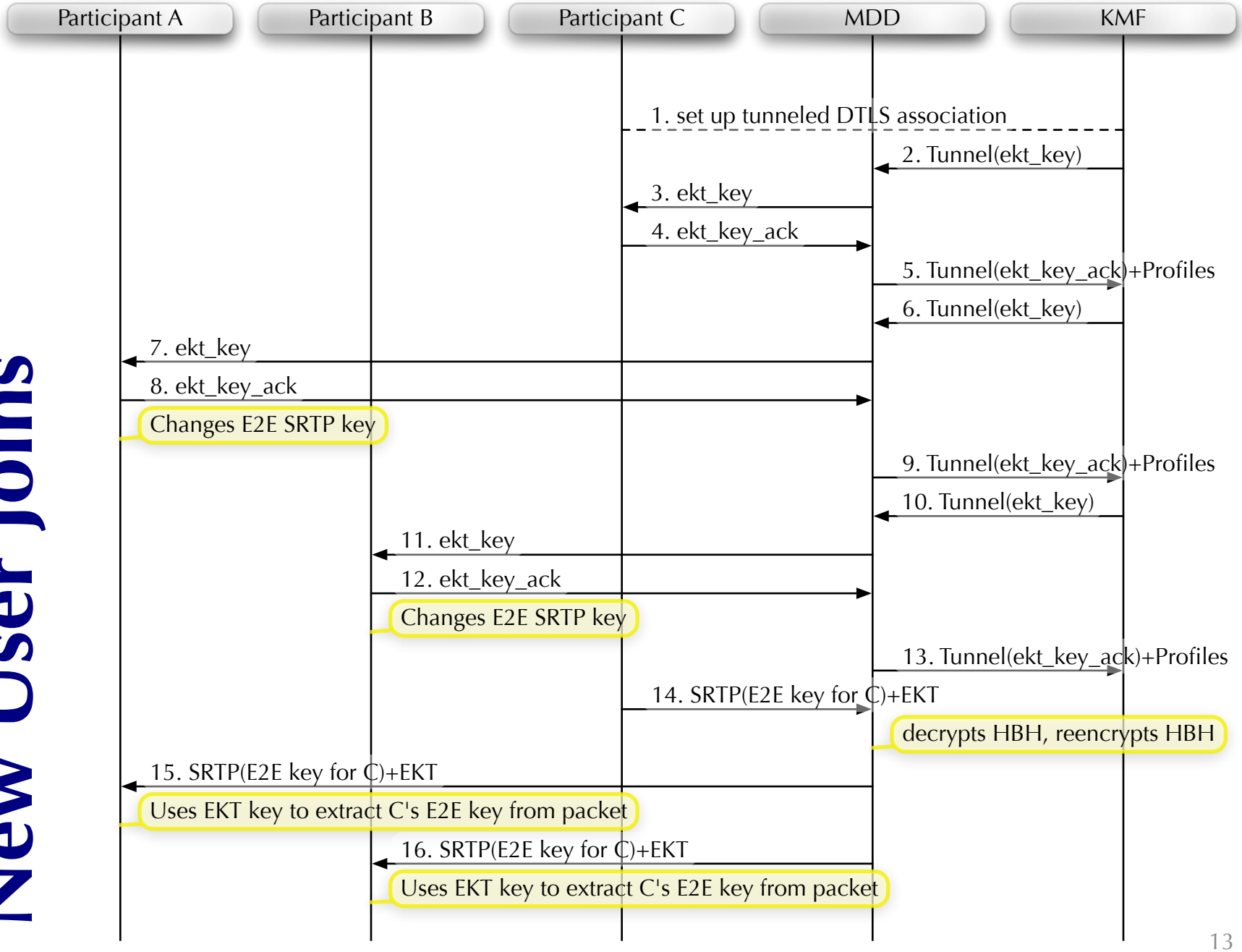
Session Setup (1/2)



Session Setup (2/2)



New User Joins



Note: Steps 2-5 happen in parallel with steps 6-9 and 10-13.