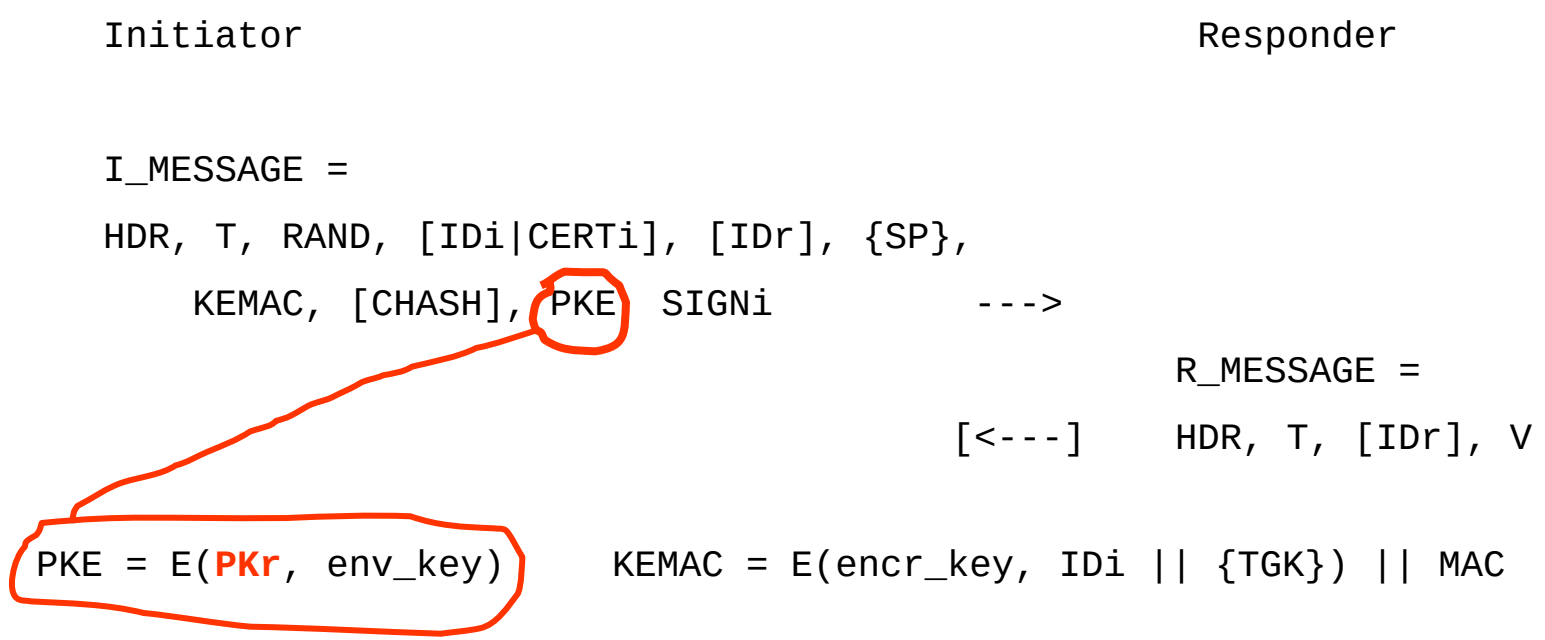
An additional mode of key distribution in MIKEY

draft-ignjatic-msec-mikey-rsa-r-00

D. Ignjatic, L. Dondeti, F. Audet

Public key in MIKEY (RFC 3830)

- MIKEY Public key mode requires initiator to have responder's Public key (PKr) before sending the I_MESSAGE

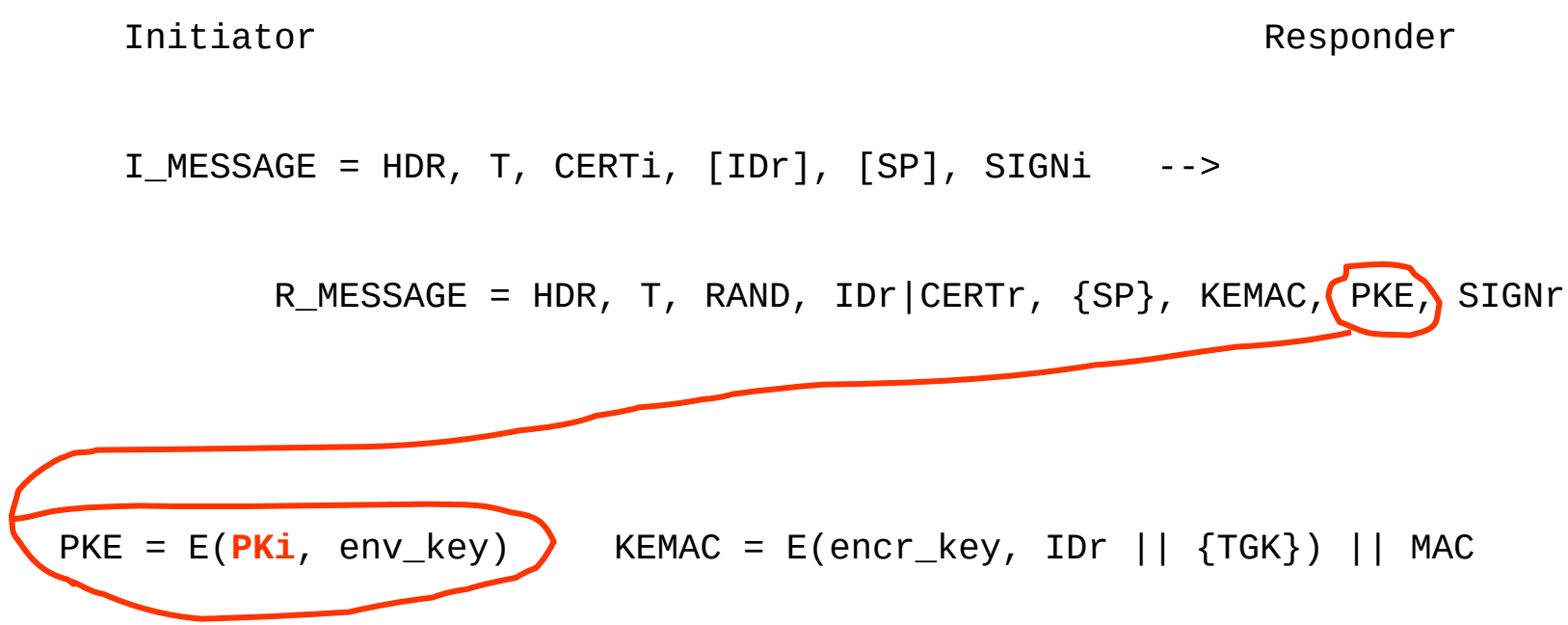


Problem description

- Very often, one does not have the PKr in advance, especially for peer-to-peer communication such as SIP
  - Certificate of responder may not be known in advance
  - Can not use MIKEY Public Key mode
- Responder may have different identity than one originally called
  - Calls may be made to “group aliases”, phone numbers for hunt groups, etc.
  - “Forking” or “retargeting” (SIP for “forwarding”)
  - Can not predict who will answer
  - Will result in multiple round-trips
- You may still want to do media encryption (sRTP) in those cases

Proposed solution

- New MIKEY Mode
- Responder generates TGKs and PKE



I_MESSAGE

- Presents public key/cert of initiator to responder
- Includes Timestamp (T) for replay protection
- Responder’s Identity (IDr) optional
  - Indicating who initiator is interested in talking to
- I_MESSAGE signed (SIGNi) to protect against DOS
  - Entire MIKEY message

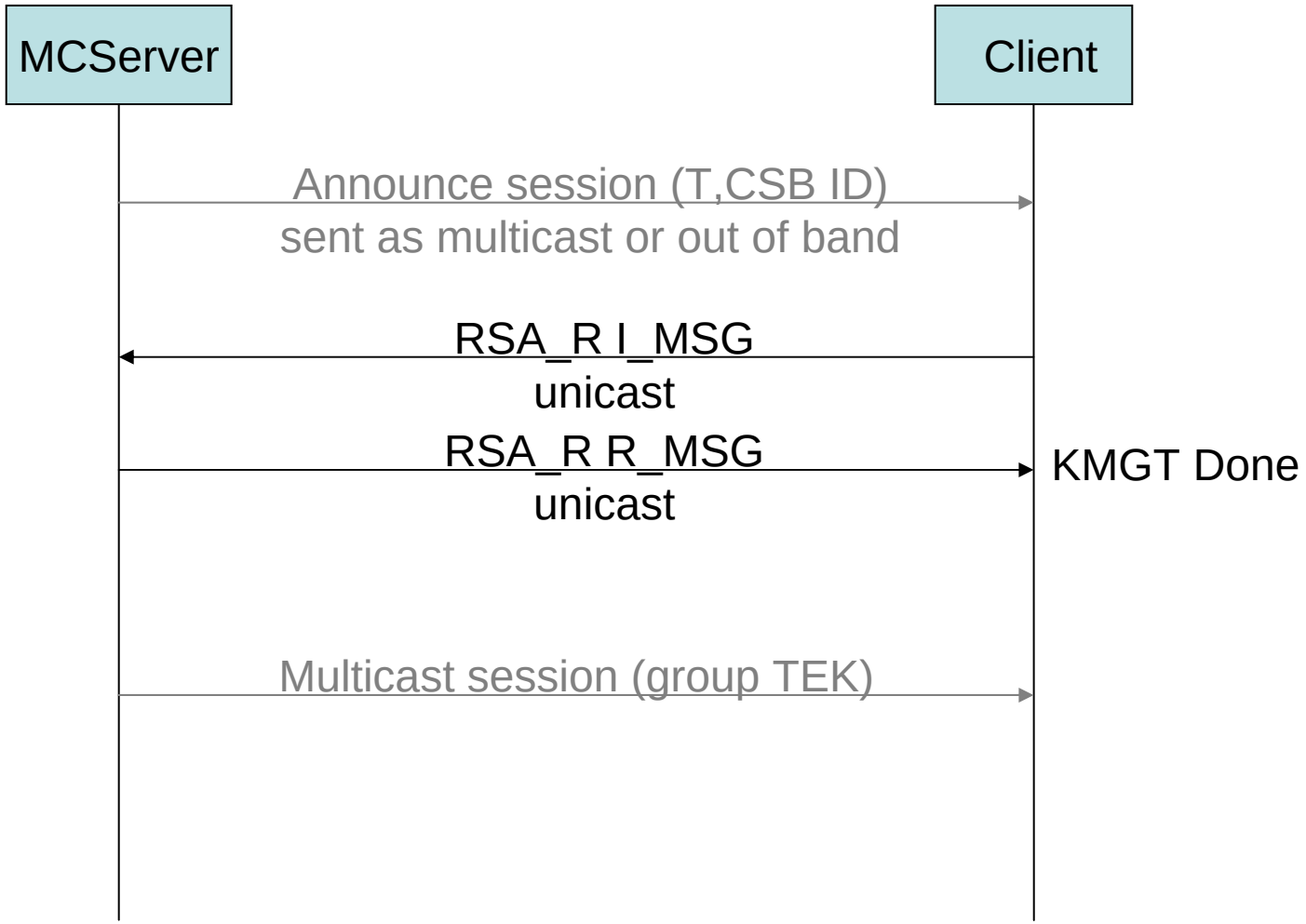
R_MESSAGE

- Full roundtrip to download TGKs
- PKE encrypted with Initiator public KEY (PKi)
- KEMAC includes encrypted Identity of responder (IDr) & TGKs, plus a Message Authentication Code (MAC)
- Also includes responder CERTr or IDr if there is reason to believe that CERTr is already provided using other means

Other

- Initiator may decide to proceed or not by based on identity/certificate of responder
- New mode especially useful when expecting retargeting, forking, etc.
  - When you still want media encryption (sRTP)
- Traditional mode useful when NOT willing to accept retargeting (i.e., when only wishing to reach a specific known user)

Use of MIKEY-R with multicast



Conclusion

- Open issues
  - Describe multicast conferencing
  - Describe 3-way calling with identical media steams
- Proposal:
  - Accept new MIKEY mode as working group document