EAP Extensions for EAP Re-authentication Protocol

draft-ietf-hokey-rfc5296bis-04

Qin Wu
Zhen Cao
Yang Shi
Baohong He

Outline

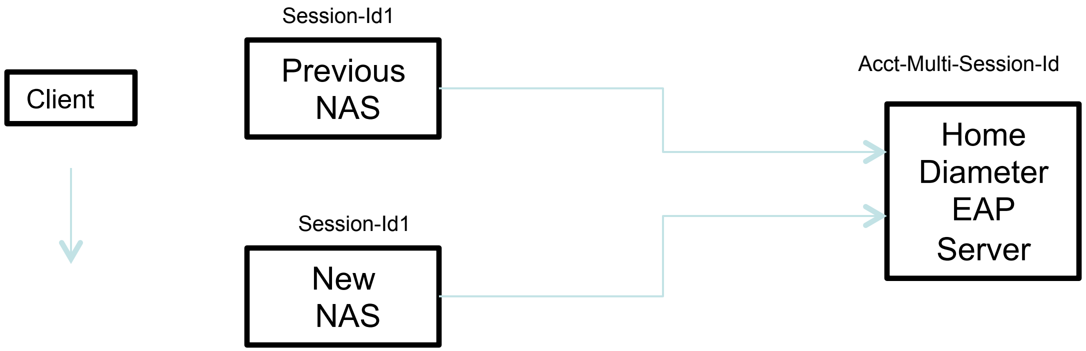
- Changes
- Issues
- Moving Forwarding

Changes since previous version

- Explain why SHOULD is implemented instead of using MAY in section 5.3.1.1.
- Keep local and home distinction in accordance with last meeting consensus
- Separate the last two paragraph as independent bullets in section 8.
  - Prevent DoS attack
  - Keying materials Transport
- Simplify Implicit bootstrapping and Explicit bootstrapping
  - Keep 'B' flag in the ERP Initiate message
  - Allow ER authenticator respond to the peer directly without forwarding the ERP message to the home domain

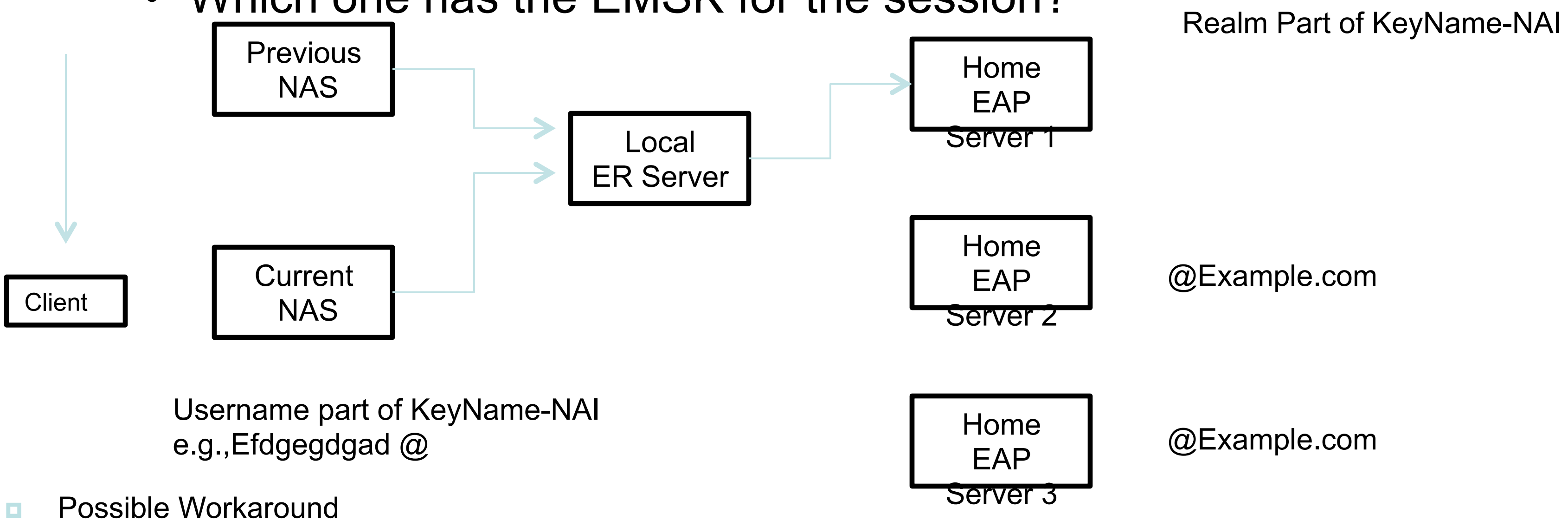
Issue from Diameter ERP

- Session Management during Peer handover
  - Is the session considered a new session each time handover?
    - Yes: different Session-Id, new Authorization, …
    - No: problem with server-initiated messages
      - When the peer move to the new authenticator, how does the server know this and send the message to the new authenticator?
      - Possible way to solve this is to register the new location of the new authenticator each time peer moves.
    - In both cases, problem with accounting if there is no constant unique identifier to identify session during handoff
    - Possible workaround: Using Acct-Multiple-Session-Id to treat the sessions during handoff as the same session



Issue from Diameter ERP

- Multiple EAP servers located in the same home realm
  - Finding the right EAP server for bootstrapping
    - Which one has the EMSK for the session?



Realm Part of KeyName-NAI

@Example.com

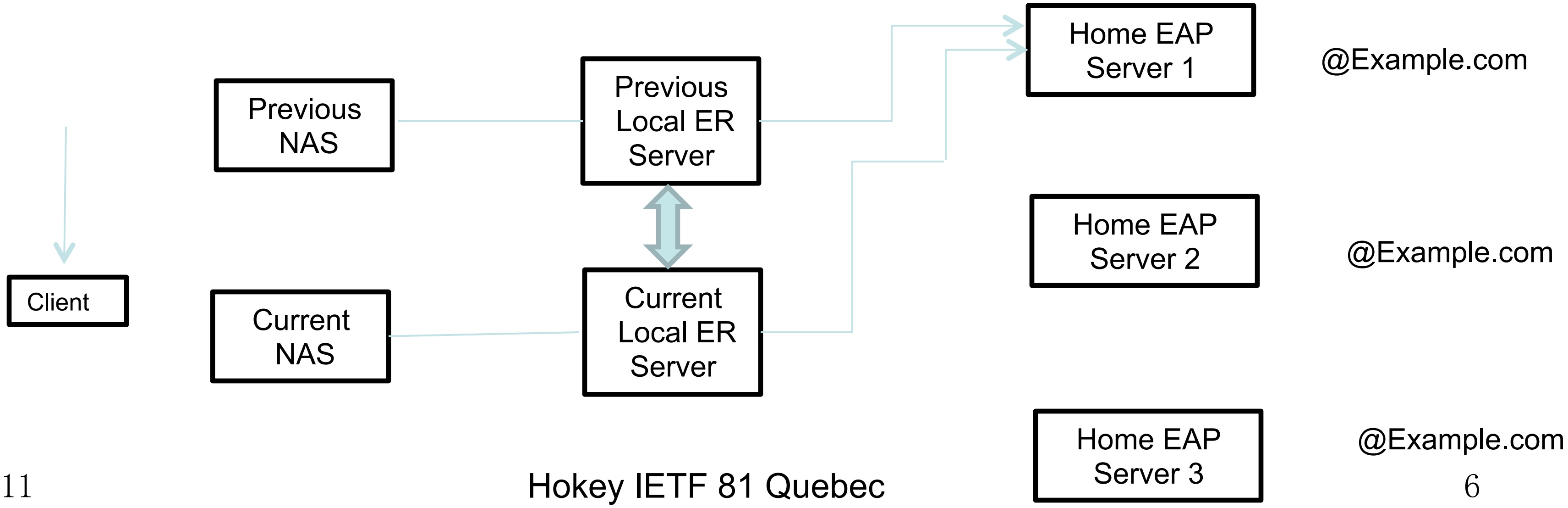
@Example.com

Username part of KeyName-NAI
e.g.,Efdgegdgad @

- Possible Workaround
  - Allow multiple EAP severs located in the home realm (1)
    - Not specific to Diameter ERP application since various home EAP servers can not be distinguished using the same real name.
    - Even Using Decorated NAI can not reach the right Home EAP server
    - Allow local ER server to save the the home EAP server name if all NAS share the same Local ER server
  - Only allow one home EAP server located in the home realm (2)

Issue from Diameter ERP

- Multiple EAP servers located in the same home realm
  - New issue arises when we allow multiple local ER server located in the same visited realm
    - When the client handover from previous local ER server to the new local ER server, Previous local ER server save home EAP server name but current Local ER server haven’t saved home EAP server name.
  - Possible workaround
    - Possible way to fix this is to allow previous Local ER server inform other ER server in the same visited domain about home EAP server name.



Moving Forward

- Known issue waiting for being addressed
  - remove Explicit bootstrapping case
  - Limit use of ERP in the visited domain or local domain
- Encourage more review of draft and early feedback