Can a Local ERP Server Be Separated From a Diameter Proxy?

An Architectural Exploration

Tom Taylor

091110

Introduction

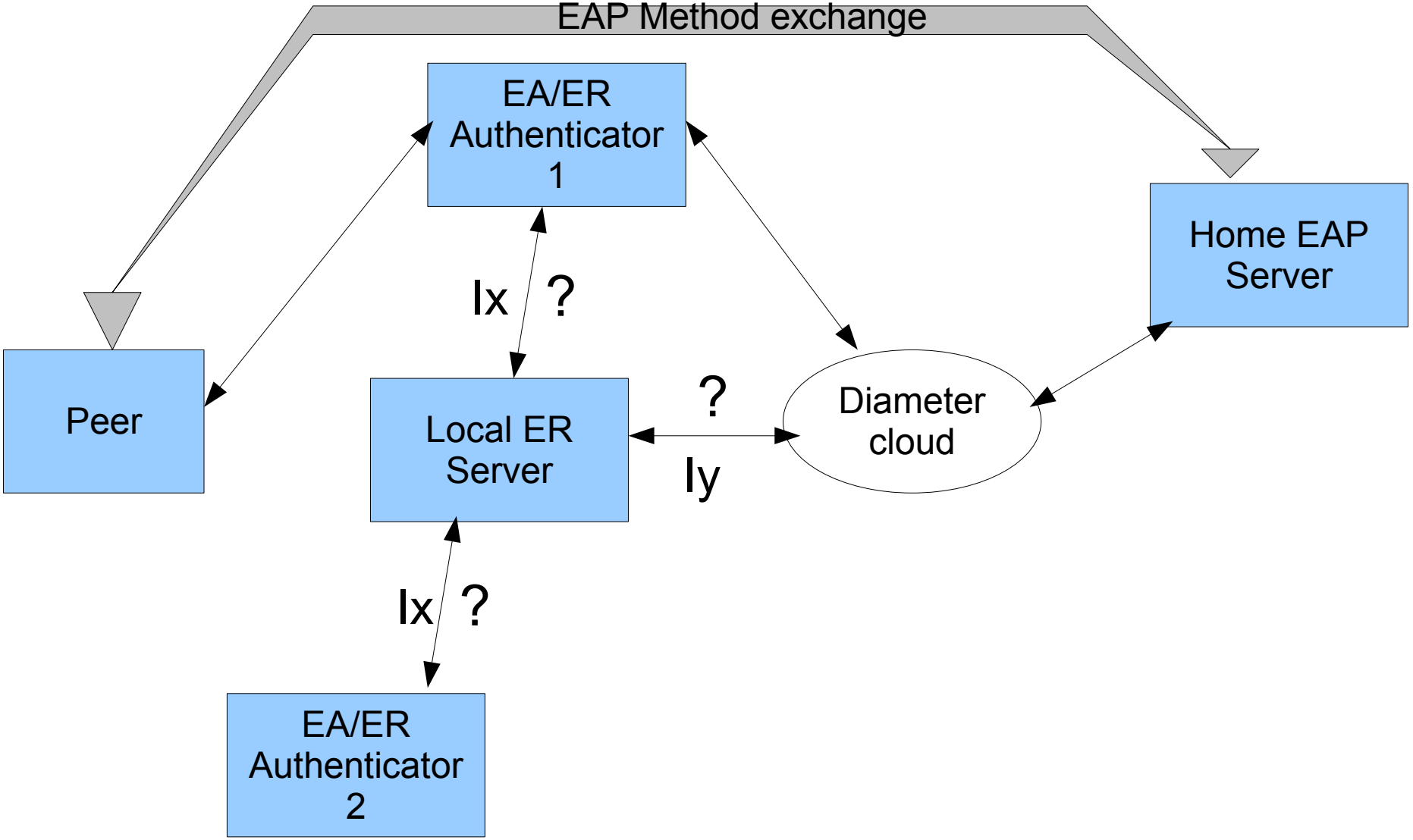
This presentation was inspired by discussion of the ERP application in DIME.

- A number of difficult architectural points have been raised.
- The discussion is just about the local ERP server collocated with a Diameter proxy, as described in RFC 5296.
- This presentation explores what would be required to support a stand-alone local ERP server.

This presentation draws no conclusions. It simply raises the question:

Is it feasible to have a stand-alone local ERP server?

Initial EAP Authentication Phase, per RFC 5296 Figure 3 modified



It seems very probable that **Iy** is required, both for direct ER server to EAP server interaction for authorization and for consistency with RFC 5296 collocation case during authentication. **Ix** is a possible alternative.

Information Flows Required During Initial Authentication Phase

- Following on RFC 5296, need a request for DSRK to go to the EAP server and the DSRK to come back to the local ER server.

- Need DSRK to be associated with a correlator (e.g., user identifier) that will be present in signalling in the reauthentication phase so the DSRK can be retrieved when needed.

Possible Solutions – Initial Authentication Phase

Alternatives:

(1) Local ER server advertises the EAP application (or maybe a new EAP relay application). EA/ER Authenticator 1 sends the original EAP authentication request to the local ER server, which adds a request for DSRK and relays to the home EAP server. The local ER server extracts the DSRK from the response and relays the rest to the authenticator. All messaging via **ly**.

(2) EA/ER Authenticator 1 sends request to home EAP server, receives response, sends DSRK to local ER server via **lx** or **ly**. This is consistent with RFC 5296 in terms of the messaging seen by the home EAP server but requires new authenticator behaviour.

(3) EA/ER Authenticator 1 does ordinary EAP authentication with home EAP server, then sends trigger message with correlator to the local ER server via **lx** or **ly**. The local ER server requests the DSRK and receives the response.

Information Flows Required During Re-Authentication Phase

- Authentication signalling must pass from the peer through EA/ER Authenticator 2 to and from the local ER server.
- The correlator established during the initial authentication has to be presented with the new signalling.
- If there is more than one local ER server, either all must share the DSRK from the initial authentication or there has to be a way to locate the right one.
- A separate authorization step is probably required.

Possible Solutions – Re-Authentication Phase

- Basic information flow seems obvious:
  - Local ER server advertises the ERP application. EA/ER Authenticator 2 sends the re-authentication request to the local ER server, which carries out reauthentication with the peer. All messaging via **ly**.
- Routing problem might be solved by depositing cookie with the peer during initial authentication. Peer sends it back. Problem is that the cookie has to be understood by entities other than the originator.
- Concerns with accounting, home network awareness of new point of attachment, authorization can be resolved by subsequent authorization exchange between local ER server and home network.