AAA Support for ERP

draft-gaonkar-radext-erp-attrs

draft-dondeti-dime-erp-diameter

IETF-70, Vancouver, Dec 2007

Topics

- ERP message transport via RADIUS/Diameter
- DSRK Request and Delivery
- How to protect the delivery?

Carrying ERP Messages over AAA

- This part is easy
- ERP messages are carried just as any other EAP messages
- There are some straightforward details
  - NAS copies rIKName-NAI TLV or the peer-id TLV from EAP Initiate Reauth into User-Name attribute/AVP
- Specification of which ERP messages are carried in which AAA messages

Key Transport

- rMSK is transported just as the MSK is transported
  - <duck for cover>
- For DSRK transport, specify/use a RADIUS attribute
  - That’ll work for Diameter also
  - This was the advice from Bernard, Glen, and others

How to Protect Key Delivery

- The RADIUS WG is considering two solutions for this
  - RADIUS keywrap
  - DTLS
- Diameter message protection
  - IPsec
  - TLS
- It’s hop-by-hop in most cases
  - But …
  - Yeah, there are contractual agreements that SPs are comfortable with