AAA Support for ERP

draft-gaonkar-radext-erp-attrs

(draft-dondeti-dime-erp-diameter)

IETF-71, Philadelphia, PA

Topics

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

Carrying ERP Messages over AAA

- This part is easy
- ERP messages are carried just as EAP messages
- There are some straightforward details
  - NAS copies keyName-NAI TLV from EAP-Initiate/Re-auth into User-Name attribute/AVP
  - Specification of which ERP messages are carried in which AAA messages
- Where unspecified, 3579 rules apply.

Key Transport

- rMSK is transported using RADIUS-keywrap
  - Specify EAP rMSK as 2 (although it may be ok to reuse EAP MSK assignment for it)
- For DSRK request and delivery use RADIUS-keywrap
  - draft-zorn-radius-keywrap
  - That'll work for Diameter also

DSRK Request using Keywrap

Type	Length	Reserved	Enc Type
App ID = EAP DSRK (number TBD)			
KEK ID = <NULL>			
KM ID = NULL@domain-name			
Lifetime = <NULL>			
IV = <NULL>			
Data = <NULL>			

Enc Type = 0 implies the use of AES-KW;
The request does not need to be encrypted!

DSRK Keywrap

Type	Length	Reserved	Enc Type
App ID = EAP DSRK (number TBD)			
KEK ID = KEK_ID			
KM ID = EMSKname@domain-name			
Lifetime = Lifetime			
IV = IV			
Data = DSRK			

Questions?