Diameter Attribute-Value Pairs for Cryptographic Key Transport

draft-wu-dime-local-keytran-02

Qin Wu

Glen Zorn

Diameter Attribute-Value Pairs for Cryptographic Key Transport

- Objective
  - specifies a set of Attribute-Value Pairs providing native Diameter support of cryptographic key delivery
- Motivation
  - Update RFC 4072 Diameter EAP application to use more generic grouped AVP to carry different cryptographic keys
  - Support not only Diameter EAP application but also Diameter ERP application
  - Compatible with AVP defined in the RFC4072

Diameter Attribute-Value Pairs for Cryptographic Key Transport

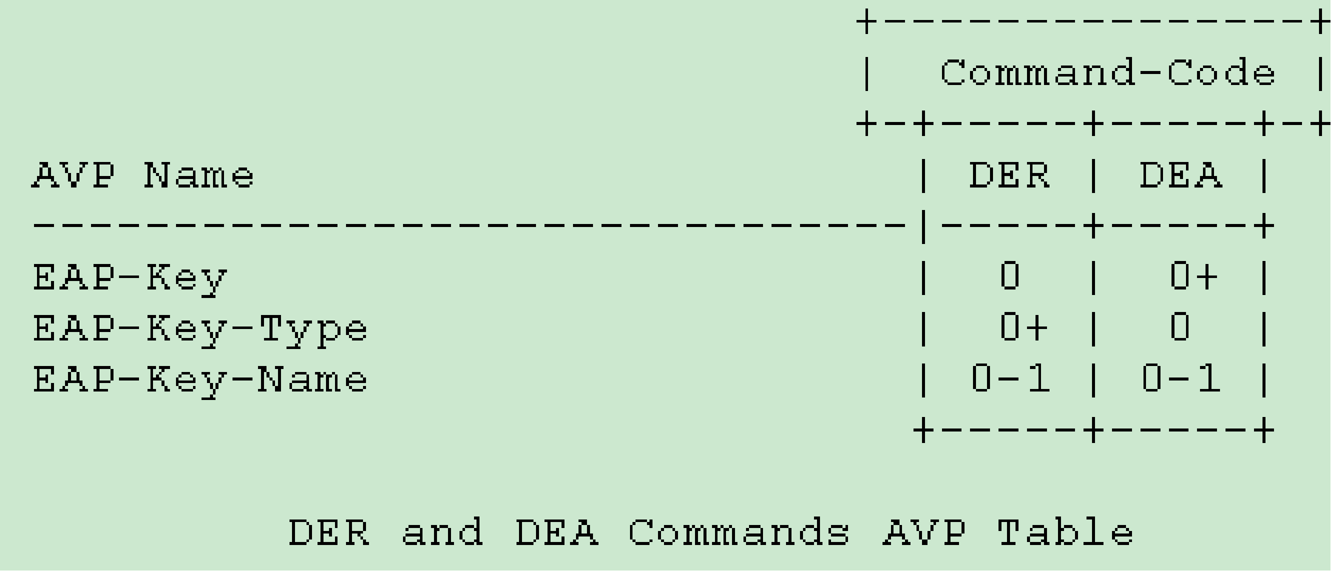
- EAP-Key AVP

```
EAP-Key ::= < AVP Header: AC1 >
          { EAP-Key-Type }
          { EAP-Keying-Material }
          [ EAP-Key-Lifetime ]
          [ EAP-Key-Name ]
          * [ AVP ]
```

- EAP-Key-Type AVP
  - of type Enumerated containing MSK(0),DSRK(1),USRK(2),rRK(3),rMSK(4),DSUSRK(5)
  - included in a DER command as a signal that a certain type of key is required in the response (e.g., to support ERP)

Diameter Attribute-Value Pairs for Cryptographic Key Transport

- EAP-Key-Name AVP
- EAP-Keying-Material AVP
- EAP-Key-Lifetime AVP



	Command-Code	
AVP Name	DER	DEA
EAP-Key	0	0+
EAP-Key-Type	0+	0
EAP-Key-Name	0-1	0-1

DER and DEA Commands AVP Table

Proposal

- Adopt it as WG work item?

Thanks

www.ietf.org