Enctype Negotiation

Larry Zhu
Microsoft Corporation
IETF 62

Draft Status

- draft-zhu-kerb-enctype-nego-00.txt
- Extension: Client-server negotiation of enctype
- Implementations: LH beta1, Heimdal

Enctype Negotiation Extension

- Client send enctype list via authorization-data in AP-REQ.

  AD-ETYPE-NEGOTIATION 129

  EtypeList ::= SEQUENCE OF Int32 -- the client's proposed enctype list in decreasing -- preference order, favorite choice first

- Wrapped in IF-RELEVANT

Enctype Negotiation Extension cont’d

- Server selects an enctype supported by both the client and the server
- The chosen enctype is then sent in the subkey field of AP-REP

Questions?