KDC Referrals

Larry Zhu
Microsoft Corporation

IETF 60

Goals

- Remove costly client side configuration

Draft Status

- Latest revision
  - draft-ietf-krb-wg-kerberos-referrals-04.txt
- Two client side interoperable implementations available

Updates

- PA-SERVER-REFERRAL-DATA contains the realm name for the next TGS request
- solution to the GNU FTP problem
  - Using an alias “GNUFTP” to request a ticket for ftp.gnu.org, outside of administrative boundary

Open Issues

- Ticket and referral info mix&match attack
  - Several solutions possible
    - PA-SERVER-REFERRAL-DATA contains the key to decrypt the enc-part of the TGS reply, - as done in PKINIT
    - Include the AS_REQ nonce in PA-SERVER-REFERRAL-DATA, to bind the referral info with the reply (and the request), – proposed by Ken
    - Move it into the enc-part, - extensions

Next Steps

- Call for consensus on the draft going to last call