YAP

Kurt.Zeilenga@lisode.com
Design Considerations

- Password-based, simple user names (flat name space, no realms)
- Rely on TLS to secure authentication exchange and subsequent application data exchange
- Internationalization
- Identity Assumption Support
- Hash agility
- KISS
  - Easy to specify
  - Easy to understand
  - Easy to implement
Exchange Overview

- Start TLS
- Negotiate Mechanism
- C->S: <message>
- S->C: provide outcome
Details

- message = authzid separator [ authcid ] separator data
- where data is produced by
  \[ \text{HMAC( ChannelBindings,} \]
  \[ \text{Concat( authzid, authcid,} \]
  \[ \text{HMAC( UTF8( SASLprep( password )), authcid))} \]
- Server stores either the password or the inner HMAC (password equivalent).