Mutual Auth – status update

- News since last London meeting
  - -algo draft is now WG draft
  - PBKDF2 introduced as password hardening
    - Standardized: PKCS #5 2.0, RFC 2898
    - Possible better alternatives exist, but no standards
- Tracker issues
  - Closed: 6/8 issues
  - Remaining 2 issues:
    - #4: will be incorporate in the next draft
    - #9: solution proposal sent to ML

Mutual Auth – status update

- Elliptic Curve issues
  - Ilari's suggestions for non-cofactor-1 curves
    - To be incorporated in –algo-01 draft
  - "NIST curve" issues: my plan
    - Wait TLS WG – CFRG curve discussions for consensus
      - Currently TLS WG asking CFRG for curve choice suggestions
    - If the answer is "NIST curve OK", do nothing; else,
    - If suggestion accepted by TLS-WG before *our deadline*:
      - Incorporate as a default parameter
    - If suggestion not accepted before our deadline:
      - Publish using current NIST curves
      - Supplement by another draft, or update on next chances