Issues in “A SASL and GSS-API Mechanism for Oauth”

http://datatracker.ietf.org/doc/draft-ietf-kitten-sasl-oauth/

Why do we now have HTTP formatted SASL messages in the draft?

- The current draft is based in it's first instance on the Google XOAUTH mechanism which uses an HTTP formatted message to as the message format.
- XOAUTH supports OAuth 1.0a which has a very specific signature requirement based on multiple elements form an HTTP request. Using an HTTP format allows this to lean heavily on the OAuth 1.0a documentation and extant implmetations without introducing new complexities.
- Oauth 1.0a signatures have proven hard to reliably implement, so adding complexity there is probably not a good idea.

What can we do instead?

- Several folks have asked for a simpler message format, comma or CRLF separated in the style of many other SASL mechanisms.
- This makes sense because parsing HTTP is by all reports VERY hard to do right.
- We would need to provide enough data fields to support the currently known data requirements for the various OAuth authentication token profiles and a mapping.
- Extensibility so that new profiles can specify additional data elements.

Sizing up the options…

- HTTP format
- PRO
  - Very close to a successful extant implementation.
  - Leans heavily on the other specifications without changes.
- CON
  - Parsing HTTP correctly and fully is VERY hairy.
  - Potentially very overweight payloads if client isn't careful/minimalist.

- Simplified format
- PRO
  - Much easier to parse
  - Somewhat lighter weight
- CON
  - Requires implementers to properly deal with the mappings.
  - Extensibility needs to be done right.
  - Discovery information return changes completely.

Other Issues

- Current inline endpoint discovery
  - Very lightly reviewed
  - Does not match or support anything like the Simple Web Discovery initial draft and doesn’t interoperate with it.