A SASL Mechanism for OAuth
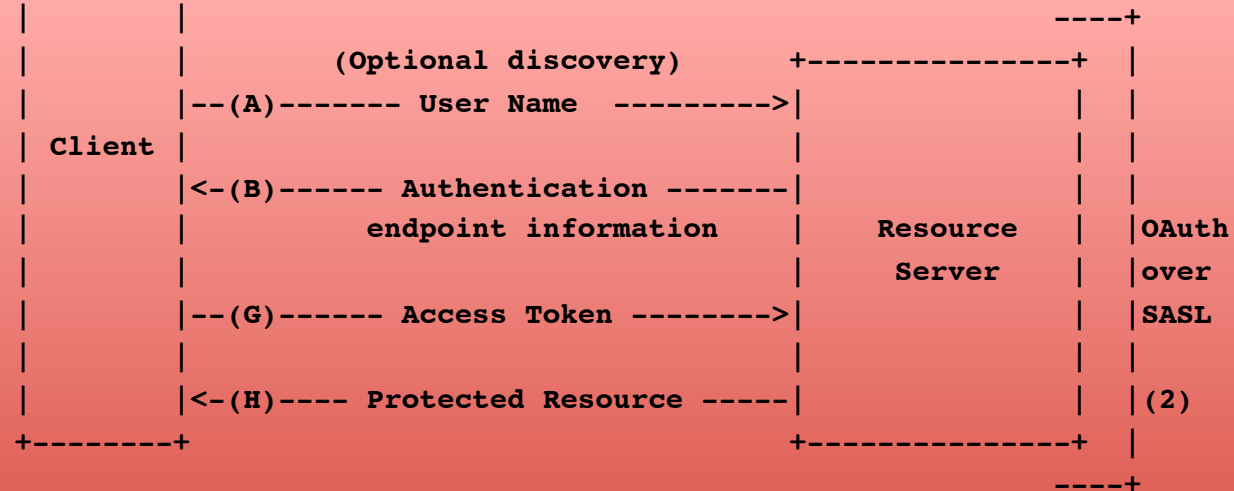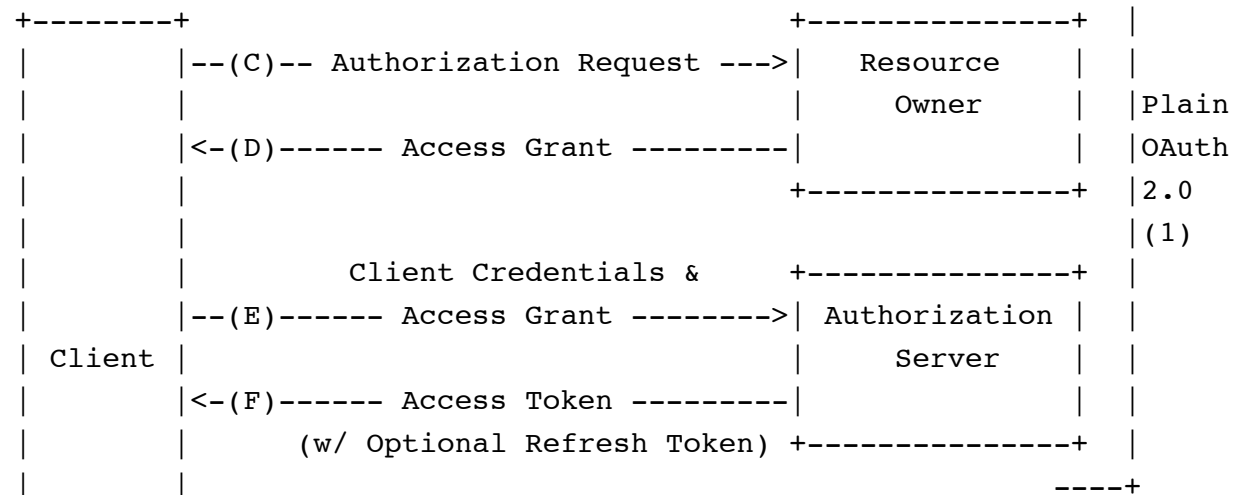
draft-mills-kitten-sasl-oauth-00.txt

W. Mills, T. Showalter, H. Tschofenig

Overview

```
+--------+                               +--------------+  |
|        |--(C)-- Authorization Request --->|   Resource   |  |
|        |        |                        |     Owner    |  |Plain
|        |<-(D)------ Access Grant ---------|              |  |OAuth
|        |        |                        +--------------+  |2.0
|        |        |                                          |(1)
|        |        |   Client Credentials &    +--------------+  |
|        |--(E)------ Access Grant -------->| Authorization |  |
| Client |        |                        |     Server   |  |
|        |<-(F)------ Access Token ---------|              |  |
|        |        | (w/ Optional Refresh Token) +--------------+  |
|        |        |                                        ----+
|        |        |
```

```
                                              ----+
|        |        |   (Optional discovery)    +--------------+  |
|        |--(A)------- User Name  --------->|              |  |
| Client |        |                        |              |  |
|        |<-(B)------ Authentication -------|              |  |
|        |        |   endpoint information  |   Resource   |  |OAuth
|        |        |                        |    Server    |  |over
|        |--(G)------- Access Token -------->|              |  |SASL
|        |        |                        |              |  |
|        |<-(H)---- Protected Resource -----|              |  |(2)
+--------+        |                        +--------------+  |
                                              ----+
```

Example

```
S: * IMAP4rev1 Server Ready
C: t0 CAPABILITY
S: * CAPABILITY IMAP4rev1 AUTH=OAUTH
S: t0 OK Completed
C: t1 AUTHENTICATE OAUTH
R0VUIC8gSFRUUC8xLjENClVzZXI6IHNjb290ZXJAYWx0
YXZpc3RhLmNvbQ0KSG9zdDogaW1hcC55YWhvby5jb
20NCkF1dGhvcml6YXRpb246IFRva2VuIHRva2VuPSJ2R
jlkZnQ0cW1UYzJOdmIzUmxja0JoYkhSaGRtbHpkR0V1
WTI5dENnPT0iDQoNCg==
S: +
S: t1 OK SASL authentication succeeded
```

Open Issues

- How strongly should the draft map to the Google implementation?
  - http://sites.google.com/site/oauthgoog/Home/oauthimap
- How strong does the OAuth signature mechanism needs to be re-used?
- Is a bearer token-based support useful/needed?
- Channel binding support needs to be discussed

Next steps?

- Open issues need to be clarified
- Working on this document in the KITTEN group?