A SASL Mechanism for OAuth

draft-mills-kitten-sasl-oauth-00.txt

W. Mills, T. Showalter, H. Tschofenig
Overview

![Diagram of OAuth 2.0 flow]

---

1. **Authorization Request**
   - Client sends an Authorization Request to the Resource Owner.
   - Resource Owner responds with an Access Grant.

2. **Access Token**
   - Client requests an Access Token from the Authorization Server.

---

(Optional discovery)

---

- **User Name**
  - Client sends User Name to the Resource Server.

- **Authentication**
  - Client sends Authentication and endpoint information to the Resource Server.

- **Access Token**
  - Client requests an Access Token from the Resource Server.

- **Protected Resource**
  - Client requests a Protected Resource from the Resource Server.

---

2.0

(1)

Plain

OAuth

(2)

SASL

over

over
Example

S: * IMAP4rev1 Server Ready
C: t0 CAPABILITY
S: * CAPABILITY IMAP4rev1 AUTH=OAUTH
S: t0 OK Completed
C: t1 AUTHENTICATE OAUTH
R0VUIC8gSR5hUC8xLjENC1VzZXI6IHNjb290ZXJAYWx0
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](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?