OAuth Profile for Open Public Clients

https://datatracker.ietf.org/doc/draft-ietf-mailmaint-oauth-public/

Neil Jenkins

Current flow

1. Email → Autoconfig file
2. Autoconfig file → protocols + endpoints + OAuth issuer identifier
3. Issuer identifier → Open OAuth flow

Proposed flow

1. Email → Autoconfig file
2. Autoconfig file → protocols + endpoints

PACC

---

3. Endpoint → RFC 9728 Protected Resource Metadata
4. Resource metadata → OAuth issuer identifier
5. Issuer identifier → Open OAuth flow

Open OAuth

Well-known path

https://api.example.com/jmap/session

https://api.example.com/.well-known/oauth-protected-resource/jmap/session

WWW-Authenticate

GET https://api.example.com/jmap/session

401

```
WWW-Authenticate: Bearer
  resource_metadata="https://api.example.com/.well-known/
  oauth-protected-resource/jmap/session"
```

Non-HTTPS

Scopes
Semantic vs Protocol

`urn:ietf:params:oauth:scope:mail`	`imap / pop / smtp / jmap`
`urn:ietf:params:oauth:scope:contacts`	`carddav / jmap`
`Urn:ietf:params:oauth:scope:calendars`	`caldav / jmap`

Next steps