User Managed Access (UMA): Protocol

**UMA - Step 1. User registers Host at AM**

**HOST** (as Client for 1st OAuth)
- Provision of AM location
- Construct host-meta url

**AUTHORIZING USER** (End-user at browser)
- Retrieve host-meta metadata
- Learn about User Authorization URL (OAuth end-user authz. endpoint)

**AUTHORIZATION MANAGER** (as Authorization Server)
- Metadata document

1st OAuth: Web server client profile

**1st OAuth - Step 1. Obtaining end-user authorization**
- [Redirection of end-user user's agent to end-user authz. endpoint] Client Identifier & Redirect URI
- User authenticates & decides on access request
- [Redirection to Redirection URI] Authorization Code

**1st OAuth – Step 2. Obtaining an Access Token (HOST ACCESS TOKEN)**
- Client Credentials & Authorization Code & Redirect URI
- Validate Authorization Code
- Access Token (w/ optional Refresh Token)
- Optional registration of scopes
User Managed Access (UMA): Protocol

UMA - Step 2. Requester gets access token from AM

HOST (as Resource Server for 2nd OAuth)

AUTHORIZATION MANAGER (as Authorization Server for 2nd OAuth)

REQUESTER (as Client for 2nd OAuth)

Access request

Unauthorized, Location of AM

2nd OAuth: Autonomous client profile (there is no Step 1)

2nd OAuth – Step 2. Obtaining an Access Token (REQUESTER ACCESS TOKEN)

Request for Access Token (Client credentials, optional scope)

Evaluate against applicable policy

Alt

Access Token (w/ optional Refresh Token)

Unsuccessful access token response

Claims-required document

Submit claims
User Managed Access (UMA): Protocol

UMA - Step 3. Requester wields access token at Host to gain access

HOST (as Resource Server for 2nd OAuth)

AUTHORIZATION MANAGER (as Resource Server and Authorization Server for 1st OAuth) (as Authorization Server for 2nd OAuth)

REQUESTER (as Client)

2nd OAuth – Step 3. Accessing a protected resource

Access request with (Requester) Access Token

1st OAuth – Step 3. Accessing a protected resource

Request validation of Requester access token (send both Requester access token and Host access token)

Validate access token

Token validation response

Alt

Local token validation

Resource

Unauthorized

1st OAuth: Web server client profile

2nd OAuth: Autonomous client profile

© Fraunhofer