Step 1: User introduces Host to AM (UMA-specific profile of an "embedded" WRAP instance)

Legend: **UMA term is bold and purple / WRAP term is bold italic and orange**

**Host** as **Client** seeking user authz to use this **AM** as the **Authz Server** for its resources protected on behalf of this user

a. Provision **AM** location

b. Construct hostmeta URL

c. Retrieve hostmeta and learn user authorization URL

d. Engage in any user delegation profile to authz this **Host/Client** to respect this **AM** (and optionally access its **Protected Resource** later in Step 3)
Step 2: Requester gets access token (UMA-specific extension/profile of ordinary WRAP)

Legend: **UMA** term is bold and purple / **WRAP** term is bold italic and orange

**AM** as **Authz Server** of record for the **Protected Resource** below

- **Host** as **Protected Resource**
  - **Protected Resource**

- **Authorizing User** as **Resource Owner** of resource at **Protected Resource**
  - a. Provision resource location
  - c. Ask for access token, supplying claims as demanded

- **Requester** as **Client** seeking access to resource at **Protected Resource**
  - b. Attempt access on user-delegation basis (if there is a requesting person) or autonomous-client basis and get sent to **AS**

- Person on whose behalf **Requester** is acting
UMA protocol over WRAP-friendly substrate
Step 3: Requester uses access token to get to resource (UMA-specific extension)
Legend: UMA term is bold and purple / WRAP term is bold italic and orange

AM as Authz Server of record for the Protected Resource below

b. (optional) Wield access token from Step 1 to approach token validation URL to get token presented by Requester validated

Host as Protected Resource

Authorizing User as Resource Owner of resource at Protected Resource

a. Attempt access, wielding access token from Step 2

c. Give access

Requester as Client seeking access to resource at Protected Resource

Person on whose behalf Requester is acting