

User Managed Access Core Protocol

Logical testcases based on User-Managed Access (UMA) 1.0 Core Protocol¹

Step 2: Requester gets access token from AM

Actors: Requester, AM

Preconditions

Requester has the role Oauth client

AM has the role Oauth Authorization Server

Conformance mode

..

Substeps

The following substeps are performed in order to achieve Step2:

- 1 Requester attempts access resource at host
- 2 Requester visits AM's requester_token_uri endpoint
- 3 Interaction AM and Requester (combination Core step2, substep3and4)

Step2Substep1: Requester attempts access resource at host

Description:

see User-Managed Access (UMA) 1.0 Core Protocol step 2

requester(Oauth client) seeks requester access token from AM (OauthAuthorization Server)

result: requester is given AM's requester_token_uri endpoint

Steps per SP/IP (here UMA different): ..

OverallSTEP2Branch1:

IF Requester is acting on behalf of requesting party
AND (requesting party = Corporation OR requesting party = other legal person
OR requesting party = natural person NE authorizing user)

THEN Requester MUST use UMA profile pattern not involving Oauth end-user authorization

OverallSTEP2Branch2

Else IF Requester is acting on behalf of requesting party
AND (requesting party = natural person EQ authorizing user)

THEN Requester MUST use UMA profile pattern involving Oauth end-user authorization

Substep2step1: Requester attempts to access resource at host

Step2Substep1Step1Branch1

IF (requester knows AM's access token URL AND requester did not first approach host)
THEN requester MAY go direct to URL

Step2Substep1Step1Branch2:

ELSE requester MAY go direct to resource at HOST

Step2Substep1step1Branch3:

IF (requester attempts access resource at host WITHOUT access token)
THEN HOST responds with challenge:
"http 401 unauthorized" Code AND HTTP header "WWW-Authenticate'contains
requester_user_uri endpoint)

Failing element: requester

Substep2: Requester visits AM's requester_token_uri endpoint

Teststeps submit HTTP-request using the GET method and desired scope to access token URL still in development/Rework , see 7th paragraph Step 2 page 7 UMA Core protocol??

Description:

seeUser-Managed Access (UMA) 1.0 Core Protocol: step 2
Requester visits AM's requester_token_uri endpoint
result: requester provides its desired scope

Steps per SP/IP (here UMA different): ..
watch branches (IFs)

Teststeps submit HTTP-request using the GET method and desired scope to access token URL

Substep3 Interaction AM and Requester

Test2Substep3Branch1 (Happy flow)

IF requester performs a HTTP-request using the GET method on access token URL
AND HTTP request contains (HTTP " accept header")

THEN

IF AM requires NO claims for grant authorization based on user policy
THEN AM response EQ (Oauth access token response + possible refresh token URL)

Test2Substep3Branch (error)

ELSE

IF requester NOT authorized according to user policy
THEN AM response EQ unsuccessful Oauth access token response
AND authorization negotiation ends (**How??, CONFORMANCE-ISSUE**)

Failing element: requester

Test2Substep3Branch

ELSE

IF AM requires more info based on user policy from requester
THEN AM response EQ claims-required response containing claims-req. List
AND List SHOULD make use of media type (indicated acceptable by requester)

Test2Substep3Branch

IF requester receives from AM a claims-required list
THEN requester performs HTTP-request using the POST method to authorization negotiation URL
AND HTTP-request contains claims document
AND type claims-document specified in " content-type" header
THEN type claims-document can be recognized by AM

AND AM accepts document

AND AM gives response (see above) OR AM gives another claims-derived response (**IN DEV?. CONFORMANCE-ISSUE**)

Test2Substep3Branch (error)

IF requester receives from AM a claims-required list
THEN requester performs **HTTP-request using the POST method** to authorization negotiation URL
AND HTTP-request contains claims document
AND type claims-document NOT specified in " content-type" header

THEN type claims-document can NOT be recognized by AM

AND AM rejects document

AND AM GIVES ERROR RESPONSE (**??, not specified, CONFORMANCE-ISSUE**)

Failing element: requester

