User Managed Access Core Protocol

Logical testcases based on User-Managed Access (UMA) 1.0 Core Protocol[i]

Step 3: Requester wields access token at host to gain access (REQS INCOMPLETE, CONFORMANCE-ISSUE)

Overall description:

User-Managed Access (UMA) 1.0 Core Protocol p.8

Preconditions
Requester has the role Oauth client
Host has the role of Oauth resource server
Host has to contain a protected resource
AM has the role of Oauth Authorization Server

Conformance mode

Substeps

The following substeps are performed in order to achieve Step3:

1. Requester attempts access
2. host asks AM to validate requester access token
3. AM validates response and gives response

Step3Substep1: Requester attempts access (the protected resource at the host)

short Description:

Step3Substep1Branch1:

IF requester presents to host request access token (issued by AM in Core Step2) by means of process described in section 5 Oauth[ii] **(Further testdescription nec.?)**

AND request misses Access token
THEN request is invalid AND host issues invalid_request error
AND host does not proceed (HOW?, **CONFORMANCE ISSUE**)

Failing elemenr= Requester
ELSE host proceeds (HOW??, **CONFORMANCE ISSUE**)

Step3SubStep2: host asks AM to validate requester access token

short Description:

host sends requester access token to AM's token verification endpoint by POST-message

Step3Substep2branch 1:

IF format message ok, req. Acc. Token in message, IP address requestor's request in message
THEN POST Success (Description POST message, see UMA 1.0 Core Protocol, prg 3)

Step3Substep3: AM validates response and gives response

*Step3Substep3*branch1
IF AM determines token is valid
THEN AM sends (JSON-document in HTTP) response with 200 OK status
AND response contains list of scopes applying to PART. REQ. ACC. TOKEN
and host validates the scopes OK
THEN host gives access in manner as described in scopes to requester

*Step3Substep3*branch2
else
IF AM determines token is invalid
THEN AM sends 'invalid_requester_token'error response to host (FORMAT in dev. **CONFORMANCE-ISSUE; error response as described for Oauth??)**
AND host returns 'invalid token response to requester (section 5.2.1 Oauth2 protocol, Hammer-Lavav)

Failing element: AM

*Step3Substep3*branch3
else
IF AM determines token is expired
THEN AM sends 'expired_requester_token'error response to host (FORMAT in dev.; **CONFORMANCE-ISSUE; error response as described for Oauth??**)
AND host returns 'invalid token response to requester (see section 5.2.1 Oauth2 protocol, Hammer-Lavav)

Failing element: requester

*Step3Substep3*branch4
else
IF host validates the scopes: 'insufficient scope'
THEN host returns 'insufficient scope error' to requester(FORMAT in dev.; **CONFORMANCE-ISSUE; error response as described for Oauth2??**)
Failing element: requester

*Step3Substep3*branch5
else
IF host validates requestor's request badly formed
THEN host returns 'invalid_request'error to requester(FORMAT in dev.;

CONFORMANCE-ISSUE; error response as described for Oauth2??)

Failing element: requester

*Step3Substep3*Branch6
else
IF host token validation request badly formed
THEN AM returns 'invalid response'error to host(FORMAT in dev.;
CONFORMANCE-ISSUE; error response as described for Oauth2??)

Failing element: Host

---

i https://github.com/mrtopf/UMA-Specifications; version-date: 4-12-2010
ii Hammer-Lahav, E., "The OAuth 2.0 Protocol," 2010.