UMA V2.0 Disposition of Comments

FINAL

Introduction

The User-Managed Access (UMA) Work Group's UMA V2.0 Draft Recommendations have undergone two Public Comment and IPR Review periods, the first 25 May 25 - 12 July 2017 and the second 28 Sep - 12 Nov 2017. This document records the group's disposition of comments received for the entire period 25 May to 12 Nov.

Key

- **Comment Reference:** The GitHub repository issue number of the comment and possibly a reference to a subpart of that issue. All issues relevant to the Public Comment and IPR Review period use both the label "V2.0" and the label "public comment period". The content of all comments has been stored in GitHub.
- **Issue Description:** Characterization of the issue in a short phrase. May be different from the issue name in GitHub.
- **Specification Reference(s):** A reference such as "Grant Sec *n.n*" or "FedAuthz Sec *n.n*", indicating *actual sections* that were edited. "Grant" refers to User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization revision 05 and "FedAuthz" refers to Federated Authorization for User-Managed Access (UMA) 2.0 revision 05, the Draft Recommendations under review in the case of the first Public Comment period for most of the comments, or in the case of the final *n* issues, User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization revision 08. Issues relevant to each specification were labeled "grant" and "fedauthz", respectively. Some new sections were added and some sections were rearranged in the course of editing, but only rev 05/rev 08 section numbers are used so that commenter references will be normative.
- **Editorial/Technical:** Whether the comment involves an editorial change (a change to interpretive wording, generally minor) or a technical one (a change to normative language that requires substantive specification change). A label of "editorial" was applied to issues that appeared, at first blush, to be editorial. Note that applying these categories itself requires interpretation, and there is some gray area between them. **Implementers seeking to understand changes and to develop conforming UMA implementations are encouraged to study all changes carefully.**
- **Disposition:** The Work Group's conclusion about the action to take in response to the comment. "Commit" links go to specific GitHub commits showing exact specification text changes.
- **Report Out:** Whether the commenter submitted comments through the official Public Comment period channel, and requires reporting back of the disposition. Kantara staff should take action on this column.
- **Notes:** Context that may be helpful for the Leadership Council.

Comment Reference	Issue Description	Specification Reference(s)	Editorial/ Technical	Disposition	Report Out	Notes
#326	Improve and reorder definition of permission ticket	Grant Sec 1.3	Editorial	Commit		Editorial improvement to a spec definition suggested, agreed by WG, and implemented.
#327	Rationalize usage of "object" vs "parameter" labeling	Grant Sec 3.3.6	Editorial	Commit		Simple editorial wording fix suggested, agreed by WG, and implemented.
#328	Interpreting how client-contributed scopes are mapped to resources during authorization assessment	Grant Sec 3.3.4	Editorial	Commit		Interpretation issue raised; editorial enhancement removing ambiguity adopted by the WG.
#329	Typo: Fix cross-reference internal section target	Grant 7.4.1	Editorial	Commit		Incorrect cross-reference noted; fix applied without WG intervention required.
#330	Typo: Fix cross-reference external specification target	FedAuthz Sec 9.2	Editorial	No change		Simple editorial correction suggested; fix was overcome by events (see #334 below).
#331	Typo: Fix reference to item being registered	FedAuthz Sec 9.3	Editorial	Commit		Simple editorial correction suggested; fix applied without WG intervention required.
#332	Test whether definitions of PCT are sufficient	Grant (various)	Editorial	No change		Interpretation question raised; WG decided to keep the existing wording.
#333	Enhance `redirect_user` example	Grant Sec 3.3.6	Editorial	Commit		Simple editorial enhancement requested; fix applied without WG intervention required.
#334	Treating token introspection response claims as generic JWT claims in local token validation environments	FedAuthz Sec 1, FedAuthz Sec 9.2	Editorial	Commit		Issue raised due to lack of implementation experience; editorial resolution adopted by WG involving removal of IANA registration request section for JWT claims (meaning that claims are not yet made available for use in a formal sense inside self-contained RPTs that the RS would validate locally vs. introspect at the AS).
#335a	Distinguish UMA versions of terms from OAuth ones	Grant (various), FedAuthz (various)	Editorial	No change	Yes	Editorial improvement requested; editor recommended no change.
#335b	Spell out key UMA terms more fully	Grant (various), FedAuthz (various)	Editorial	Commit	Yes	Editorial improvements requested; small edits applied without WG intervention required.

#335c	Separate out sequence diagrams according to resource owner-side vs requesting party-side interactions	Grant Sec 1.3	Editorial	Commit	Yes	Editorial improvement to diagram(s) requested; editor recommended and implemented introductory text edits instead.
#335d	Simplify sequence diagrams, e.g. to separate claims pushing from interactive claims gathering	Grant Sec 1.3	Editorial	Commit	Yes	Editorial improvement to diagram(s) requested; added only clarification to existing single diagram after WG consultation.
#336	Clarify that RPT takes a `token_type` hint of `access_token`	FedAuthz Sec 5.1	Editorial	Commit		Editorial clarification requested, agreed by WG, and implemented.
#337a	Rationalize/complete definitions of token introspection response claims	FedAuthz Sec 5.1.1	Editorial	Commit		Clarification requested; WG determined an editorial improvement.
#337b	Clarify the situation with respect to client types in the UMA grant	Grant Sec 3.3.3	Editorial	Commit		Clarification requested; WG determined an editorial improvement.
#337c,d	Create and document a concrete method to require and enable clients to pre-register claims redirection URIs	Grant Sec 2, Grant Sec 3.3.2, Grant new Sec 7.3	Technical	Commit		Request for new mechanism for dynamic client registration mechanism and clarity; WG agreed. The new metadata field, `claims_redirect_uris`, tracks the design of a similar metadata field, `redirect_uris`, already defined by RFC7591 and registered in the OAuth Dynamic Client Registration Metadata Registry. The new metadata field requires a new IANA registration request.
#337e	Typo: Example that should show a response message is a request message	Grant Sec 3.3.3	Editorial	Commit		Simple editorial correction requested; fix applied without WG intervention required.
#337f	Clarify how permission requests with multiple permissions in them contribute to set math	Grant Sec 3.3.4	Editorial	Commit		Clarification requested; WG determined an editorial improvement.
#337g	Ensure authorization servers apply the maximum security checks on permission tickets	Grant (various)	Editorial	Commit		Additional security considerations requested; WG agreed to add a form of security considerations that gives more discretion to the authorization server than was requested.
#338	Typo: Example shows the wrong endpoint path component	FedAuthz Sec 3.2.1	Editorial	Commit		Simple typo correction requested; fixed without WG intervention required.
#339	Clarify whether an array can be used for a request for a single permission	FedAuthz Sec 4.1	Editorial	Commit		Clarification requested; WG confirmed correct interpretation and clarification text.
#340	A unique error should be available for a definitive policy-failed error	Grant Sec 3.3.6, Sec 7.4.1	Technical	Commit, commit, commit, commit		Change requested; WG reintroduced and renamed an UMA1 error code that was removed in Apr 2017: in UMA1 (see Core V1.0.1 Sec 3.5.4) was `not_authorized` and is now called `request_denied`.
#341	The `request_submitted` error should be allowed to be terminal (no permission ticket)	Grant Sec 3.3.6, Sec 5.6	Technical	Commit		Change requested to make the permission ticket optional on the AS response; WG made a different change, still requiring the ticket but adding an optional new `interval` polling hint feature. The design of the new parameter tracks the design of a similar parameter in the OAuth 2.0 Device Flow for Browserless and Input Constrained Devices (see Sec 3.2).
#342	Security considerations need to be made clearer and more to the point, especially Grant Sec 5.2	Grant Sec 5	Editorial	Commit		Clarification requested; WG determined an editorial improvement.
#343	Refer to RFC 6749 token endpoint error codes specifically	Grant Sec 3.3.6	Editorial	Commit		Clarification requested; WG agreed an explicit reference to 6749 would be helpful.
#344	Explain what to do if the client presents an invalid or expired claim token	Grant Sec 3.3.6	Editorial	Commit		Clarification requested; WG confirmed the correct interpretation and clarification text: these conditions require one of the existing errors.
#345	Explain what to do if the client presents a claim token in a format the authorization server can't handle	Grant Sec 3.3.6	Editorial	Commit		Clarification requested; WG confirmed the correct interpretation and clarification text: this condition requires one of the existing errors.
#346	*ClientedRegistered* scopes should not be a first-class set math citizen	Grant Sec 3.3.4	Editorial	No change		Clarification requested; commenter decided to close own issue without action.

#347	The authorization server should be given discretion to determine if it's an error when the client requests a scope it did not pre-register for	Grant Sec 3.3.6	Editorial	Commit		Change requested; WG broadened the authorization server's behavior, giving it discretion to report the requested error.
#348	On the refresh flow, the authorization server should be given discretion to perform authorization assessment	Grant Sec 3.3.1, Sec 3.6, new Sec 6.1, FedAuthz Sec 1.4.1, Sec 8	Editorial	Commit		Change requested; WG did not make the change but clarified that no discretion is possible. Also confirmed error and non-error cases in the RPT upgrade flow, which is like UMA-specific refreshing.
#349	Explain what to do if the client presents an invalid or expired RPT for upgrading	(see above)	Editorial	Commit		Clarification requested; WG confirmed the correct interpretation and clarification text. (See #348 above for details.)
#350	Explain what error code to return when *CandidateGrantedScopes* < *RequestedScopes*	Grant Sec 3.3.4	Editorial	Commit, commit	Yes	Clarification requested; WG confirmed the correct interpretation and clarification text, resolving several inconsistencies in the authorization assessment normative text and incompleteness in the worked example.
#351	Variety of editorial issues in FedAuthz	FedAuthz (various)	Editorial	Commit		Variety of editorial comments, typo corrections, and the like made; implemented without WG intervention required. Note that the original form of the text in Sec 3.2, since corrected, could have led implementers astray, implying that a field was required when it was clear in a different context (Sec 3.2.4) that the field would not appear.
#352	The PAT is not needed for the permission and token introspection endpoints, so use client credentials instead	FedAuthz Sec 1.4.1, Sec 1.5	Editorial	Commit		Change requested; WG made some clarifications instead.
#354-1	Explain what error code to return if the resource registration endpoint gets a request message with a bad /broken request body	FedAuthz Sec 3.2	Technical	Commit		Change requested; editor, in collaboration with some WG participants, specified the HTTP 400 (Bad Request) status code and an optional new protection-API-level error code `invalid_request`. This error code tracks the design of the similar OAuth (RFC 6749 Sec 4.1.2.1) and OAuth bearer token (RFC 6750 Sec 3.1) error codes.
#354-2	The PAT should definitively be a bearer token	FedAuthz Sec 1.3	Technical	Commit		Change requested; editor, in collaboration with some WG participants, reintroduced an UMA1 requirement to support bearer PATs (see UMA V1.0.1 Core Sec 1.4, 'The authorization server is REQUIRED to support "bearer"') whose inadvertent removal might have caused interoperability problems.
#355	Idea for the resource server to return an RPT directly rather than a permission ticket that enables a full UMA flow	Grant Sec 3.2	Technical	No change		This issue was submitted by a group participant intending for it to be an idea for a future extension, to be discussed at a later date, and the group accepted it on this basis.
#356	Typo: Add missing code example portion(s)	Grant Sec 3.3.6	Editorial	Commit		Simple editorial correction requested; fix applied without WG intervention required.
#357	Clarify set math language by removing parenthetical "clarification"	Grant Sec 3.3.4	Editorial	Commit		Clarification requested; WG confirmed the correct interpretation and action.
#358a	Concern re the authorization server being a separate service, vs. the resource server, learning requesting party PII	Grant Sec 3.3.1, 3.3.2, 3.3.4, and 6.2	-	No change	Yes	Comment requested no specific change; WG interpreted it as questioning an underlying premise of UMA and declined to take action.
#358b	Concern re claims being pushed by a client seeking access to a protected resource without authorization by the requesting party	Grant Sec 3.3.1, 3.3.2, 5.7, 6.2	Editorial	Commit, commit	Yes	Issue arose as a result of discussing alternative interpretations of #358. WG decided to add security and privacy considerations to address the concern.

Summary of Technical Changes

The following technical changes were made after the first Public Comment period. The decisions to make technical changes turned out to fall into one of two categories: reintroduce an UMA1 feature or introduce a feature that closely tracks the design of a feature already existing in OAuth or among its ecosystem of specifications. The first is important for cross-version feature parity and the second is important for the group's roadmap design priority of "simplify the protocol and make it work more like OAuth".

Issue	Description	Category

#337c, d	Added `claims_redirect_uris` OAuth Dynamic Client Registration metadata field	OAuth
#340	Reintroduced UMA1 `not_authorized` error code and renamed it to `request_denied`	UMA
#341	Added `interval` parameter to `request_submitted`; design tracks OAuth Device Flow `interval` parameter	OAuth
#354-1	Added optional `invalid_request` error code to resource registration endpoint; design tracks OAuth and OAuth bearer token error codes	OAuth
354-2	Reintroduced UMA1 requirement for PAT as bearer token to be supported	UMA

It was determined that making these technical changes necessitated returning to a second Public Comment period.