High summarization of Kantara UMA 2.0: User-Managed Access

First delivered by Eve Maler, ForgeRock, @xmlgrrl & Mike Schwartz, Gluu, @gluufederation 27 June 2018

https://www.flickr.com/photos/mrcrash/1980165121/ | CC BY-NC 2.0
User-Managed Access has important implications for those facing regulatory pressures around data protection, market pressures around consumer trust, and architectural pressures around API protection.

The following slides will offer a very high level overview of the context, purpose, structure, and flows of the UMA 2.0 protocol, including its OAuth2 extension grant and its federated authorization API.
The UMA standard’s progress

- Mar ‘15: UMA V1.0 ratified as Recommendations
- Dec ‘15: UMA V1.0.1 ratified as Recommendations
- Jul ‘17: 1st Public Comment/Review period ends
- Sep ‘17: 2nd Public Comment/Review period ends
- Jan ‘18: Final Recommendations published
- Jan ‘18: Draft UMA Business Model Report published
- Jan ‘18: Final Recommendations published
- Jan ‘18: Draft UMA Business Model Report published
- Jun ‘18: Business model/IRM
- Jan ‘18: UMA2 logo
- Feb ‘18: Charter update
- May ‘18: Vendors supporting UMA2: Gluu, ForgeRock, Keycloak (WSO2 coming Q3)

Specs refactored, over 100 issues closed, lots of implementation input received, Disposition of Comments doc written...

UMA2 logo (designed by @domcat)
OAuth is for constrained delegation to apps
It has helped to kill the “password anti-pattern”

The RO can revoke the token to withdraw authorization (consent)

Authorizes (consents) at runtime after authenticating, at the AS

App gets consent based on the API scopes it requested; it has its own identity distinct from the RO’s

Standard OAuth endpoints for authorization and access token issuance

Some number of API endpoints that deliver the data or other value-add

This can come with a refresh token for renewal without the RO’s intervention

© 2018 ForgeRock. All rights reserved.
OpenID Connect does modern-day federation
It is an OAuth-protected identity API, plus a bit more

Resource owner = Federation user
Client = Relying party
Authorization server = Identity provider ("OpenID provider")
Resource server

Along with access and refresh token, this endpoint also typically delivers an “ID token” similar to a SAML assertion

Standard UserInfo endpoint can be called with an access token to look up identity claims
User-Managed Access is for cross-party sharing

UMA brings next-gen delegation and consent to OAuth

 tinyurl.com/umawg
@UMAWG
User-Managed Access is for cross-party sharing

UMA brings next-gen delegation and consent to OAuth

Resource owner

- Ahead of time
- Anytime
- Anytime
- At run time
- After the fact

UX

- Share
- Monitor
- Withdraw
- Opt in
- Approve

Requesting party

Client

Authorisation on server

- Authorization
- Token
- Discovery
- Resource Registration
- Permission
- Token Introspection
- Claims Interaction

tinyurl.com/umawg
@UMAWG
Like OpenID Connect for *identity*, UMA adds an API *access management* layer to OAuth2

Some use cases for UMA:

• Enterprise API protection

• For financial consumers
  • Discovering and aggregating UK pension accounts and sharing access to financial advisors

• In industrial and consumer IoT
  • For proactively or dynamically sharing smart device control or data with others

• Healthcare
  • As profiled in the Health Relationship Trust (HEART) WG at OpenID Foundation
  • Part of the new OpenMedReady framework for trustworthy remote care
To sum up: UMA enhances OAuth as follows

The UMA2 Grant spec adds to OAuth2

- The resource owner authorizes protected resource access to clients used by entities that are in a requesting party role. This enables party-to-party authorization, rather than authorization of application access alone.
- The authorization server and resource server interact with the client and requesting party in a way that is asynchronous with respect to resource owner interactions.
- This lets a resource owner configure an authorization server with policy conditions at will, rather than authorizing access token issuance synchronously just after authenticating.

The UMA2 Federated Authorization spec adds to the UMA2 Grant

- Multiple resource servers operating in different domains can communicate with a single authorization server operating in yet another domain that acts on behalf of a resource owner.
- A service ecosystem can thus automate resource protection, and the resource owner can monitor and control authorization grant rules through the authorization server over time.
- Authorization grants can increase and decrease at the level of individual resources and scopes.
Walkthrough by Eve:

Sharing pulse oximeter data in a trusted and consented way with third parties through loosely coupled cloud services
Dr. Lopez prescribes a pulse oximeter to Lynda Wallace; an administrator provisions it electronically.
When Lynda first logs in to the ACME Medical patient portal, her device is inactive.
After she clicks on the red light, she is asked to consent to device activation and data reading by Dr. Lopez.
After she consents, her device now shows as active, meaning a policy is lodged to allow data sharing and her smartphone is prepared to be a hub.
After pairing the oximeter device to her phone, she logs in to her ACME Medical mobile app using the same identity credentials as on the portal.
The mobile app securely mediates an oximeter data reading, and shows that the reading was successful.
Dr. Lopez logs in to the ACME Medical portal
Dr. Lopez’s view once authenticated is this home screen
In his My Patients view, Dr. Lopez sees a listing with Lynda Wallace and others.
Dr. Lopez selects Lynda Wallace as the patient whose data he wants to view.
He chooses Lynda’s device profile
Because of the policy she consented to activate, Dr. Lopez is able to proceed to view her data.
The User-Managed Access (UMA) 2.0 grant of OAuth:

a) gives his client app a permission ticket on first resource attempt
b) requires an ID token for proof
c) issues an access token
d) requires it for data access
colin@kantarainitiative.eu

Twitter: @KantaraColin @KantaraNews

Join us at https://kantarainitiative.org/membership/
Newsletter sign-up:

https://kantarainitiative.org/reports-recommendations/