**UMA as Restatement of Agency**


Simplest OAuth flow with mappings
Attempt at UMA flow with mappings (incomplete)
Technical UMA safe harbor propositions


OAuth entities (borrowed from HEART writeup):

- Protected resource (PR): Online information or API that is access controlled through OAuth. Note that APIs can allow both “consumption of data” (read operations) and “insertion of data” (write operations) by authorized entities.
- Resource owner (RO): An entity that has OAuth access control rights to an online resource. The RO may not, however, have other “ownership” rights, such as the right to change data values within that resource.
- Authorization server (AS): An entity that issues OAuth access tokens representing the client’s authorization for access on behalf of the RO.
- Resource server (RS): An entity where the PR resides. In OAuth, the AS and RS are typically “tightly coupled” and run by the same organization (by contrast, in UMA, entities with these names might not be).
- Client: A web or mobile application (or even an IoT device) used by the RO that seeks and gains access tokens from the AS in order to access the PR. Access may be limited (scoped) to a subset of possible API operations. The RO can typically visit the AS anytime to revoke the token.

# Simplest OAuth flow with mappings

This analysis (now appearing on the GitHub wiki -- **continue discussion there, not here**) is based on the American Law Institute Restatement of the Law -- Agency Restatement (Third) of Agency (2006). https://users.wfu.edu/palmitar/ICBCorporations-Companion/Conexus/UniformActs/Restatement(third)Agency.pdf Reference terms are in **Bold**.

Let’s make the (human) RO the Principal so we can look out for their interests maximally, for now. The AS/RS is therefore the Third Party, and the C is the Agent. This is true even though the triangle hasn’t been fully formed yet.

How do we deal with parties that act as Agents for multiple parties, like “brokers”?

Should we make up “party” versions of the OAuth “entity” language, as was done in Binding Obligations?

- AS/RS, AS/RS Operator
- C, C Operator
- RO, Authorizing Party

1. AS and RS are almost certainly run by the same operator; trust between is established in some unknown fashion
2. AS gives client credentials to C -- and separately, AS/RS gives user credentials to RO (in any order)
    a. Thus, two legs of the triangle are formed. Later,the third leg of the triangle will be formed, enabling a full application of the roles we have chosen.
    b. Do we care about the “private” agreements that might have been formed for each of these two legs?
    c.
3. RO logs in to C
4. RO chooses AS/RS from C
5. C redirects RO to AS
6. RO logs in and consent to access token issuance
7. AS issues access token for C to use
8. AS redirects RO back to C (complex dance for security purposes)
9. ...eventually C gets RO back and gets access token
    a. At what point is the Agency relationship formed between the C and RO? Is this the trigger event for it? Or does it remain less fully identified? Contracts sometimes have flowcharts.
10. C uses access token at RS on behalf of RO, possibly operated live by RO or possibly with RO offline (ongoing)
    a. Are these actions similarly important for Agency status?
11. RO might revoke the access token
    a. Are these actions similarly important for Agency status?
12. ...or AS might expire the access token
    a. Are these actions similarly important for Agency status?

## Attempt at UMA flow with mappings (incomplete)

This analysis (now appearing on the GitHub wiki -- **continue discussion there, not here**) is based on the American Law Institute Restatement of the Law -- Agency Restatement (Third) of Agency (2006). https://users.wfu.edu/palmitar/ICBCorporations-Companion/Conexus/UniformActs/Restatement(third)Agency.pdf Reference terms are in **Bold**.

UMA terms are in *italics*. Eve’s attempted mapping to UMA technical constructs are in blue.

1. The unique and essential value of UMA is the ability for a **Principal** to specify a standards-based **Agent** to a **Third Party**. The UMA resource owner (RO) is the

Principal, the UMA authorization server (AS) is the Agent, and the UMA resource server (RS) is the Third Party.

2. The Third Party derives value from a “safe harbor” protection when sharing data that is under its control. The UMA RS derives value from the relationship established with the AS when the RS is releasing the data under the RS’s control.

3. The Principal derives value from the ability to delegate control to the same accountable proxy across a wide range of third parties. The UMA RO gets benefit from leveraging a single UMA AS over a wide range of (or at least multiple) RS’s. The UMA AS may also get a benefit if this is its business model (authorization-as-a-service).

4. The Principal has a direct relationship with the Third Party and can use that to introduce the Agent as well as to notify the Third Party of changes to the Agent relationship. The UMA RO has a direct relationship with the UMA RS already, independent of the AS, and the RO can introduce the RS to the RO’s AS.

5. The Principal grants **Actual Authority (3.01)** to the Agent to express assent for the Agent to act on the Principal’s behalf. The UMA RO, by virtue of authorizing the issuance of the UMA protection API token (PAT), signals its approval for the Third Party to use the Agent for resource protection (spec). The UMA RS retains the ability to protect any subset of the RO’s resources that it likes using different means or different Agents (spec).

6. The contract between the Principal and the Third Party that introduces the Agent is the ROI Form and establishes **Apparent Authority (2.03) and (3.03)** The ROI Form includes provision for **Notification (5.01)** to and by the Agent. This contract presumes a “new ROI form” that is digital. Could it encompass the PAT issuance process, for one? The PAT process could display terms and conditions on top of just the token issuance.

7. Apparent Authority ends when the Third Party that an Agent deals with is reasonably notified. **(3.11)** The process in #6 should cover this.

8. The Agent may be anyone or anything, including open source software built by the Principal. **(3.05)** How much real choice does the RO get over their choice of AS? Is it possible for a Third Party to refuse to work with a Principal’s Agent? If so, on what grounds?

9. The UMA *Requesting Party* can be a **coprincipal (3.16)** in the Agent but this would require an Actual Authority relationship between with the Agent which might compromise the Requesting Party’s privacy. The UMA requesting party (RqP) develops a similar/reciprocal, though somewhat weaker relationship with the UMA AS than does the UMA RO. E.g., the UMA RqP, by virtue of authorizing the issuance of the UMA

authorization API token (AAT), signals its approval for the [UMA client -- what is it legally?] to use the Agent for seeking and gaining authorization to the RO's recources.

10. ??? What are the UMA Client and the Requesting Party under Agency Law? Dunno.
11. The Third Party (UMA-RS) that registers an Agent (UMA-AS) deserves a **Payment (8.14)** to offset their cost in offering the API and their opportunity cost of foregoing the branding and advertising benefits of a manual Web portal that would otherwise tax the Principal's attention.
12. The Third Party is encouraged to provide a choice of Agents for Principals that don't already have one. The Agent can be changed by the Principal at any later time. This is not required by Agency Law but it would provide a large incentive for RSs to adopt UMA before someone else does.
13. ??? Can an identity provider or credential broker be a **subagent (3.15)** of the Agent as a means to protect the Requesting Party's privacy? Dunno.
14. Based on agency law and the analysis above, here is a list of the "minimum viable product" requirements for a technical protocol involving a Principal, an Agent, and a Third Party. The endpoints or parameters would be:
    a. a human-readable (PDF/HTML) version of the applicable contract (ROI Form?),
    b. agent URI or human-readable means to introduce the agent,
    c. agent choices offered by third-party for principals that don't have one,
    d. protected resource URI and human-readable name for display by the Agent,
    e. endpoints for notification of contract changes or cancellation (in both directions), including public keys to enable secure and accountable communications,
    f. endpoint to notify agent of contract activity including a description, link, or reference to the client and requesting party involved,
    g. generic contract terms including expiration date of contract, option for unilateral cancellation, read, write, or read/write transactions on the resource,
    h. an account where the RS can receive payment and a means to link payment to an authorized transaction,
    i. names and signatures of both the resource owner and the third-party.

## Technical UMA safe harbor propositions

This table is not yet in GitHub.

| Solution | Can do in UMA V1 | Can be profiled to do (e.g. in HEART) | Can be extended to do (or added to UMA V.next) | Software can add value to do | Legal and contractual solution |
|---|---|---|---|---|---|

| Proposition | | | | | |
|---|---|---|---|---|---|
| 1 Accounting for Disclosures at AS | At a minimum, only RO policy-based “attempts at access” can be captured at AS (if token was introspected by RS there), which doesn’t tackle the main “interesting” disclosures | | Even actual UMA-sanctioned access to RS resources is not strictly captured at AS, but an extension could let RS report actual accesses to AS | Systems outside UMA can access the data and throw events about it, if they wish | |
| 2. RS takes client/RqP-dependent actions on access requests | No | | | Even if client has authz, RS can choose to add non-UMA pre- or post-processing and “refuse service” (despite UMA MUST clause) | The RS is subject to business and legal constraints in this matter; access federation trust framework could specify how to do |
| 3. AS displays to RO notices that were contributed by RS that reflect RS’s statutory responsibilities to adhere to RO/RS contract, signed by RO (or AS?) | | | **Could add an endpoint/capability for registering either only a “dead” version of ROI, or elements of RS/RO contract of record, including label, endpoint for notification of changes or cancellation (in both directions), expiration date of** | | |

| | | | | | |
|---|---|---|---|---|---|
| | | | **contract, option for unilateral cancellation** | | |

The “technical propositions” are designed to be the “least intrusive solutions that will satisfy the law” without forcing the provider to confront their biases.

Accounting for Disclosures at AS: The goal is for the AS to display a list of links and date stamps (or similar un-fleshed-out information), so as to leave as much control in the RS’s hands as possible. Their concern is transparency if AfD is contemporaneous, due to claims processing procedures. AfD is actually the law, but providers say it’s too hard to achieve. Contemporaneous disclosures have a cybersecurity benefit. 99% of TPO disclosures are outside of anything the RO would have directed through policy.

RS takes client/RqP-dependent actions on access requests: If the law allows for a delay of some number of days in data transfer to the client, then the provider should have that flexibility, based on the requesting party’s attributes. Similarly, if they are required to tag the data before transferring it, or must notify a registry, all of these should be possible. In other words, a number of workflows may be required that are adjacent to the process of considering the access request.

AS displays to RO notices that were contributed by RS that reflect RS’s statutory responsibilities to adhere to RO/RS contract, signed by RO (or AS?): This would enable providers to do very little to their current processes and onboard to an UMA world smoothly. Provider motivations around FHIR: Getting more information into their domain that is currently outside their domain. “Health-ish” and quantified-self data is attractive to get hold of, and they want to compete more efficiently with the same resources.