Extending the UMA protocol to support trusted claims

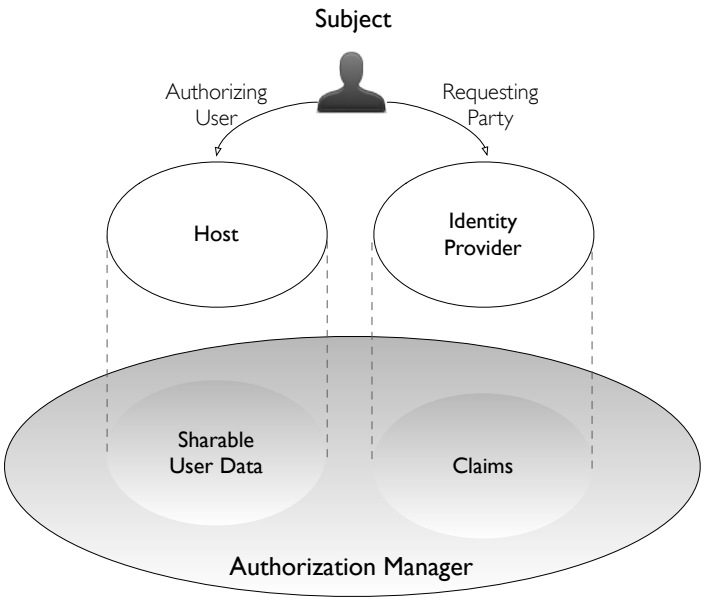
The UMA protocol supports the policy-driven ability of an AM to demand claims from a requesting party before authorization is granted. The claims may be self-asserted or third-party-asserted.
The ID Commons terminology wiki defines s claim as follows: *"An assertion made by a Claimant of the value or values of one or more Identity Attributes of a Digital Subject, typically an assertion which is disputed or in doubt."*

When claims are self-asserted (the Claimant is the Requesting Party) and the information they represent have relatively modest needs for privacy and protection, they can be handled forthrightly by means of the simple claims request/response protocol defined in UMA's requester-AM interaction. But the power of third-party-asserted claims (where the Claimant and the Requesting Party are different), coupled with potential needs to apply higher security and privacy to claims transfer, suggests a different solution.

A typical scenario involves person-to-person data sharing, in which the Authorizing User wants to restrict sharing to a specific Requesting Party identity. For such a policy to be meaningful, such a scenario often requires that the AM trust the third-party identity claim issuer.

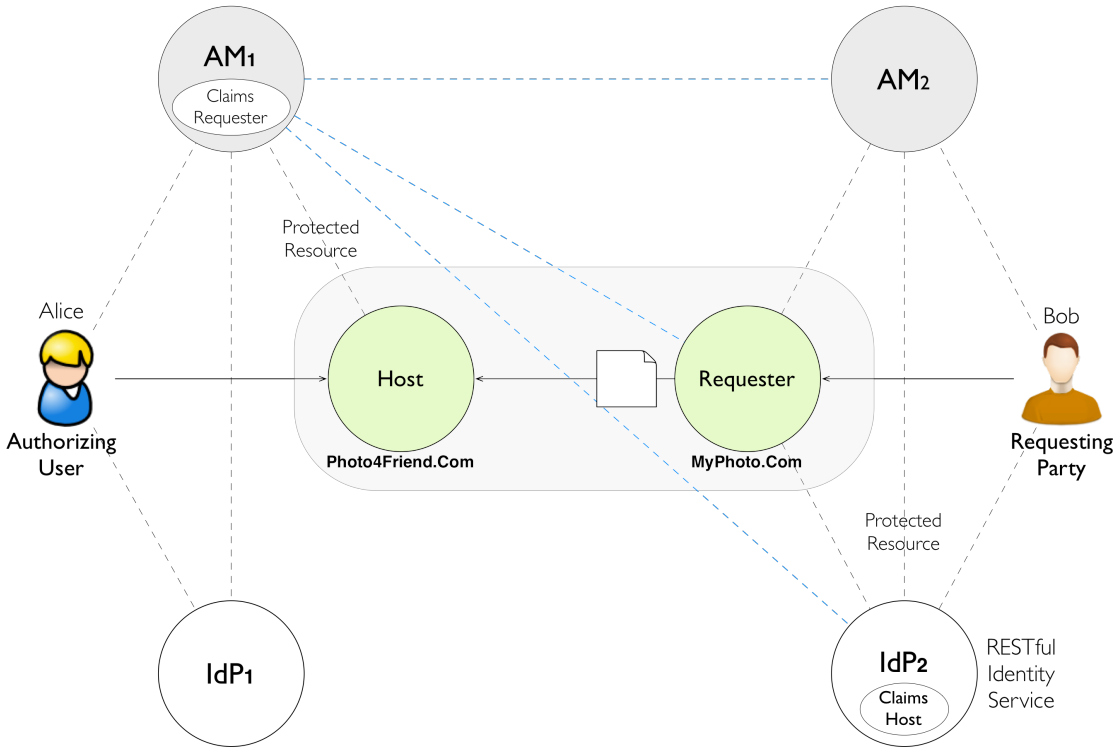
The proposed approach leverages the UMA protocol and introduces the concept of a Subject as a generic entity that refers to either the Authorizing User or a Requesting Party. Each Subject can perform actions on its own AM to authorize, respectively, arbitrary Web data sharing or the sharing of claims in support of its request to access another's Web data.

This model allows the creation of a comprehensive ecosystem in which the Authorization Manager can be used to protect both "classic" web resources and claim resources available from a Trusted Third Party (TTP) Identity Provider. The picture below shows how the subject's data is part of the UMA ecosystem.



Scenario Approach

A typical person-to-person data-sharing scenario is about photo sharing, as described and depicted in the trust relationship graph below:

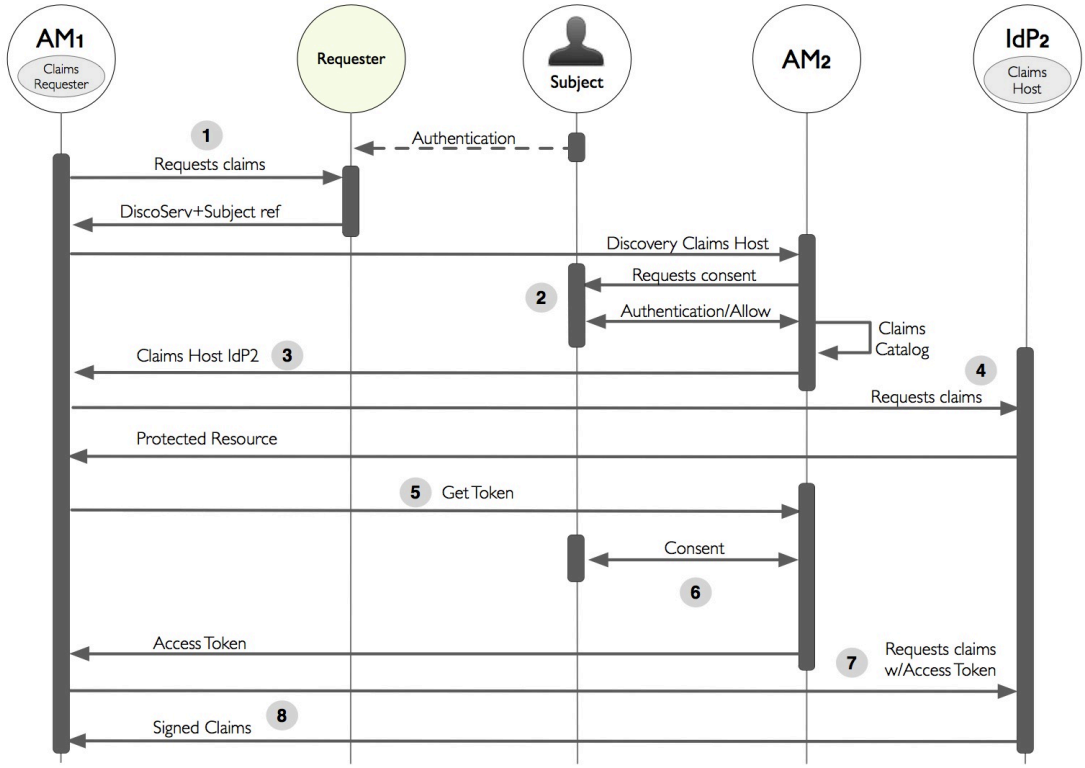


Extending this model to UMA protocol terminology, we have that:

- Alice's AM (AM_1) acts as a Claims Requester.
- Bob acts as Authorizing User for his Identity Provider (IdP_2), which acts as Host that issues claims about him.
- Bob protects his Claims Host using an AM (AM_2).

Alice wishes share a photo gallery “Sorrento photos” hosted at Photo4friend.com with Bob. She protects the gallery with an UMA Authorization Manager (AM_1), defining a policy for it that requires a specific claim "Subject/Requesting Party must have email account equal to “Bob at gmail.com”. After that, Alice sends the URL corresponding to the gallery to Bob at gmail.com.
Bob (the Requesting Party), using an UMA-enabled MyPhoto service as a Requester application, attempts to access “Sorrento photos” at Photo4friend (the Host).

Photo4friend.com redirects the Requester to AM_1 to get an access token. At this point, as the sub-sequence (high level) diagram below shows, based on Authorizing User (Alice) policy, AM_1 requires claims from the Requester (step 1). The Requester, on behalf of the Requesting Party (Bob), responds to this request not by sending the required claim directly but by informing AM_1 where the discovery claims can be found (Step 2, Step 3).

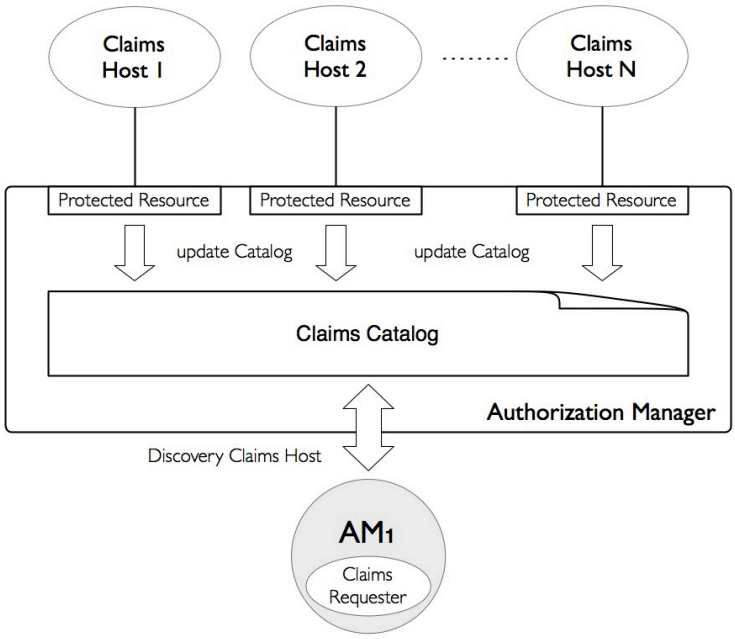


AM_1 requests claims to Claims Host/IdP_2 (Step 4). As IdP_2 is protected by AM_2, it redirect AM_1 to AM_2 to get a valid Access Token for the Claims Host resource (Step 5). In order to release the Access Token, AM_2 must verify Subject (Requesting Party) consent. In this process, the Subject must authenticate to AM_2 and express online consent (Step 6), related to the request. After that, AM_2 releases the Access Token and redirect AM_1 to Claims Host/IdP_2 (Step 7) which is able to verify the access token and returns the requested claims (Step 8).

After that, AM_1 verifies the claim document and it is able to issue an Access Token to the Requester (MyPhoto). At this point, the Requester is able to get access to the protected resource at the Host.

Claims Catalog notion

The claims catalog describes a collection of Claims host references for a Subject (Requesting Party). The claims catalog is managed and maintained at AM site. AM exposes interfaces for updating and discovery service, respectively to update the catalog from Claims hosts and to allow other AMs to discovery Subject claims host reference.



Bob must authenticate and consent in real time to discovery of claim locations, (maybe in classic UMA protocol??)

Subjects consent

Classic UMA involves Authorizing User in the protocol to express consent in the data-sharing process. The proposed model, based on reciprocal UMA scenario, moves the subject consent from the Authorizing Party to the Requesting Party. The reason is because the Trusted Claims give, implicitly, the trustworthiness about who is accessing to the protected resource at Host.

Trust Model

According to ITU-T X.509, Section 3.3.54, trust is defined as follows: *"Generally an entity can be said to 'trust' a second entity when the first entity makes the assumption that the second entity will behave exactly as the first entity expects."*

The purpose of a trust model is to respond to a specific threat profile. A threat profile is the set of threats and vulnerabilities identified through the Trusted Claims scenario.

For this particular scenario, the goal is to provide security mechanisms to handle complex inter-domain trust relationships to avoid unauthorized disclosure of Authorizing User's data.

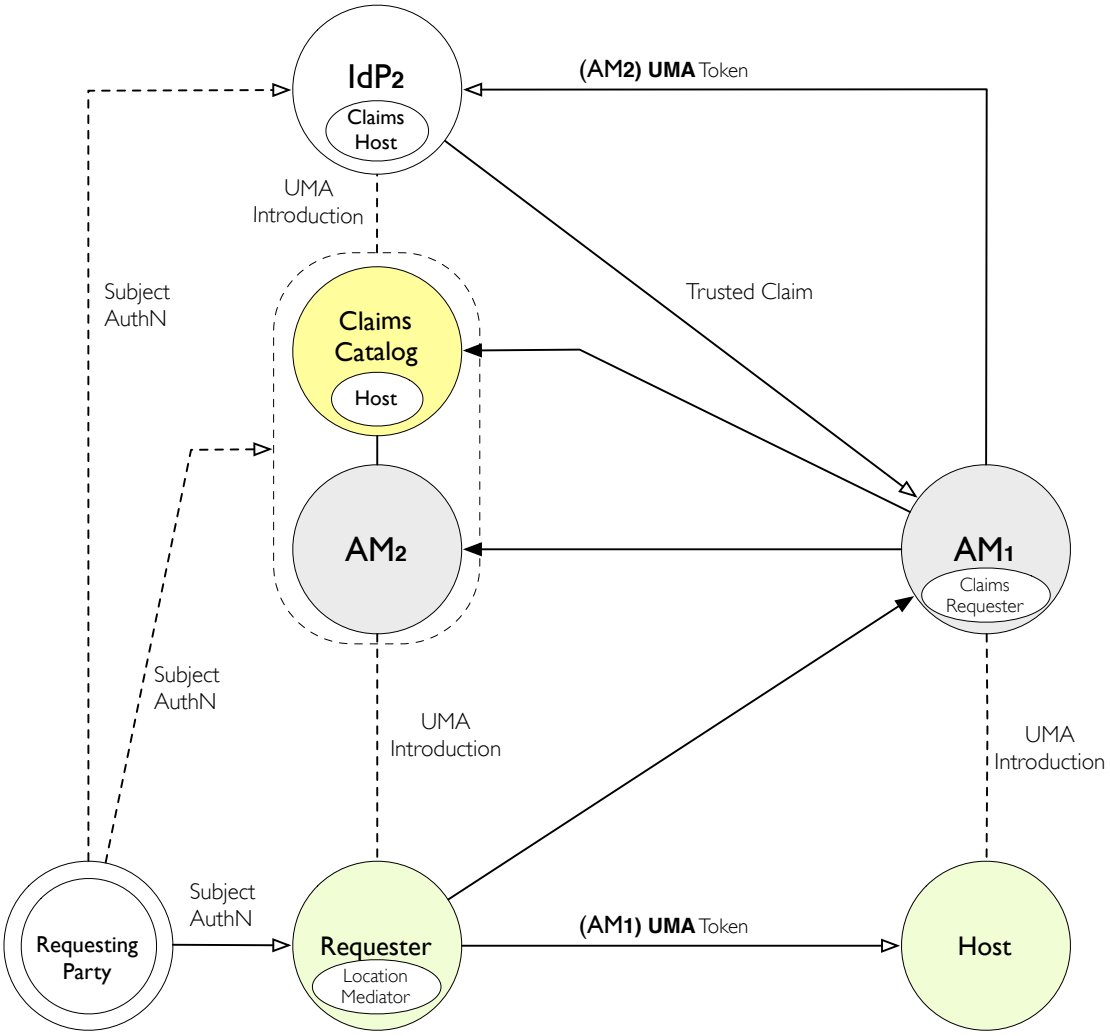
In UMA system, the trust model is defined as a set of compounded binary relationships based on individual identity or unique characteristic validation. That is, trust is the establishment of a trust relation through a validation process and the subsequent use of the relationship in the same transactional context.

There are nine different mechanisms that are present in the UMA system and are used to establish trust between different parties. These are:

- AuthN is based on the subject's identification and authentication trust.
- Website Authentication is based on such technologies as SSL/TSL where the client can authenticate the remote site it is connecting to.
- PKI-based trust relationship allows parties to build trust based on digital signatures and their verification.
- Mediator-based trust where a third party redirect capabilities on behalf of the subject.
- UMA-token builds on the possession of an access token.
- UMA-Introduction allows an individual to establish trust between two entities.
- UMA Trusted Claim – a third party asserted-claim.

Additional options which exist in this table are "Unknown" and "Untrusted". The first one exists if there is no direct interaction between parties while the second one is used when communicating parties do not have any pre-established trust relationships.

The graph below shows the chain of trust for the proposed model:



@@ trust matrix here

Bootstrapping Trust

Bootstraping trust in the UMA Trusted Claims approach leverages the notion of a Trust Framework (defined by the Open Identity Trust Framework (OITF) Model paper as *"a set of technical, operational, and legal requirements and enforcement mechanisms for parties exchanging identity information"* and sometimes called a federation) with the following goals:

- Enhance the level of assurance in the Subject's registration process at AM site.
- Create an IdP trusted network to allow the subject to control and collect centrally the set of claims from Trusted Third Party Identity Providers.

The approach to integrate UMA system with the Trusted Framework is based on the following assumptions:

- IdPs are registered with a Trusted Framework Provider (TFP) and have got a Level Of Assurance (LOA) certification.
- AM act as a Relying Party and it's registered with Trust Framework Provider (TFP) to receive notification about new certified IdP Claim Issuers.
- AM will be notified about new Claim Issuers certified by the TFP.
- AM gets the updated IdP list from the TFP (including cryptographic elements). AM provide to their Subjects a certified IdP list (with LOA certificate).
- The Subject can select a preferred IdP (Claim Issuer) to initialize an introduction process with the AM.
- The IdP (Claim Issuer) becomes a trusted and protected resource by the AM.