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 a 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) 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 it requires the AM to establish of trust of third-party identity claim issuers. [It requires transitive trust relationships: The Subject (authorizing user or requesting party) trusts its AM, AM trusts other AMs, AM trusts certified IdPs/Claims Host].

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 (AM₁) acts as a Claims Requester.
- Bob acts as Authorizing User for his Identity Provider (IdP₂), which acts as Host that issues claims about him.
- Bob protects his Claims Host using an AM (AM₂).
Alice wishes to share a photo gallery “Sorrento photos” hosted at Photo4friend.com with Bob. She protects the gallery with an UMA Authorization Manager (AM1), 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.

At this point, as the sub-sequence (high level) diagram below shows, the Subject (Bob acting as Requesting Party), using an UMA-enabled MyPhoto service as a Requester application, attempts to access “Sorrento photos” at Photo4friend (the Host), doing the following steps:

1. The Subject is authenticated by the Requester (MyPhoto).
2. The Subject fills the form inserting the protected resource link (URL) and submit the request to access.
3. The Host (Photo4friend.com) redirects the Subject to AM1 to get an access token.
4. AM1, based on Authorizing User (Alice) policy, requires claims from the Requester.
5. The Requester, on behalf of the Requesting Party (Bob), responds to this request not by sending the required claim directly but by informing AM1 where the discovery claims can be found.
6. AM1 redirects the Subject to the Claims Catalog provider (AM2).
7. The Subject is authenticated by AM2.
8. AM2 discovers Claims host provider from the Claims Catalog.
9. AM2 asks for the consent to the Subject (opt).
10. AM2 creates a session for the Subject.
11. AM2 redirects the Subject to AM1 with claims host references.
12. AM1 attempts to access to the Claims Host which is protected by AM2.
13. AM1 redirects the Subject to AM2.
14. The Subject has a valid session at AM2 (see step 7).
15. AM2 verifies consent policy for this session and redirect the Subject to AM1 with a valid access token.
16. AM1 uses the access token to access to Claims Host to get the claims.
17. Claims Host verifies the token and release a signed claims.

After that, AM1 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.
SSO Affiliated Authentication assumptions
The following assumptions SHOULD be considered in order to simplify the Subject interactions with the system components:
• Support for SSO affiliated authentication (i.e. OpenID, SAML, Infocard) in the step 1 and step 7 to allow transparent access (SSO) to the components.
• Support for Subject session management at Authorization Manager to allow caching the Subject consent.

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.

Furthermore, in order to simplify the Subject interaction with the system components, Requesting Party could specify “Silent Consent” for specific claims, which have low privacy impact. Silent Consent allows the authorization manager to release the requested claim without Subject online consent, but notifying the Subject through an out-of-band mechanism (e.g. SMS).
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:

- Subject Authentication (AuthN) verifies and confirms a Subject’s asserted digital identity based on a specific Level of Assurance (LOA). (See Bootstrapping trust paragraph below).
- 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 validation.
- UMA-token builds on the possession of an access token.
- UMA-Introduction allows an individual to establish trust between two entities and delegate authorization.
- UMA Subject consent (including notification) allows an individual to express directly consent in the authorization process for sharing data and for releasing of Claims.
- 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**

Bootstrapping trust in the UMA Trusted Claims approach is referred to the following registration processes:

- Subject registration at AM, in order to enhance the level of assurance in the Subject’s identity verification.
- Claims Host registration at AM, in order to establish trusted network to allow the subject to control and collect centrally the set of claims from Trusted Third Party Identity Providers.

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).

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

- AM is registered as Relying party with a Trust Framework Provider (TFP) to receive notification about new certified IdPs.
- AM maintains a list of certified IdPs.
• AM can act as Identity Service Provider (IdP) in case it is certified from a TFP.

The diagram below shows the interaction relationship among the actors for the Subject and Claims Host registration processes.

**UMA Subject Registration at AM**
UMA Authorization Manager (AM) provides three subject registration functions:
1. Simple Self-registration (no level of assurance)
2. Trusted registration
3. Affiliate registration

AM Self-registration provides a simple registration form to allow a Subject to create an account on a UMA system.

Trusted registration is involved when the UMA AM service is also a certified Identity Service Provider from the TFP. In this case the UMA AM service provides a valid mechanism to verify user identity and credentials coherently with its Level of Assurance.

Affiliate registration is based on trusted third party identity service provider (LOA certified), which provides subject’s identity information through identity federation mechanisms (OpenID, SAML, PIV-I, etc.). Automatically, an affiliate registration produces a Claims Host provider entry in the Subject’s Trusted claims profile.
**Trusted Claims Host Registration at AM**

UMA Authorization Manager (AM) provides a Trusted Claims Host registration process by which a Subject is allowed to register a specific Identity Service Provider from a list of LOA certified IdPs, as Claims Host.

The registration process includes the following steps:

1. The Subject selects an Identity Service Provider from a list of LOA certified IdPs that AM is able to maintain.
2. The Subject is redirect to the selected Identity Service Provider site where is requesting to authenticate and validate to the necessary IdP level of assurance.
3. After that, IdP returns the subject’s identity attributes (no value) to AM which registers them with the Subject’s Trusted Claims profile.
4. The Subject can manage identity attributes for claims settings (request online consent, notification, audit, etc.).