Identity-Hub

Towards the Identity in the Cloud

Mikaël Ates - mates@entrouvert.com - Research Engineer

Entr'ouvert - www.entrouvert.com - www.identity-hub.com

15th, february, 2011

Identity in the Cloud?

"*Identity in the Age of Cloud Computing: The next-generation Internet's impact on business, governance and social interaction*", J.D. Lasica, ASPEN roundtable gathering 28 leaders and experts in ICT - Summer 2008:

"The group tended to agree that a user-centric open identity network system is the right approach at this point. It could give everyone the opportunity to manage their own identity, customize it for particular purposes, (i.e., give only so much information to an outsider as is necessary for them to transact with you in the way you need), and make it scalable across the Net. Other ways of looking at it include scaling the social web by allowing the individual to have identity as a kind of service [...]"

Outline

From “user-centric architectures” to “an identity-centric Internet”

Two mains issues

Why an online rich user environment is conceivable

Which protocols?

Identity-Hub

Conclusion

Outline

User-centric architectures

- User control on the dissemination of personal data, certified and self-asserted.
- Samples of user-centric architecture and protocols: SAML, IDWSF, Infocard, OpenID, OAUTH, UMA works.

Identity in the Cloud?

- Identity as a service : user-dedicated identity management online services:
  - authentication server,
  - digital credential (certified identity attributes) management,
  - journal of personal data disseminated,
  - analyze policies,
  - etc.
- All the user services are accessible whatever terminal a user employs, no data on terminals.
- The user terminal may only be provided with a standard Web browser (so we consider here only Web technologies).

Identity-Centric Internet

A rich online environment :

- Every entity, person, network or organization, is provided with an online environment to manage the storage and access control to its personal (resp. organizational) data.
- Let's call this environment an **Identity in the Cloud Agent** (IC-Agent).
- An IC-Agent simultaneously assume multiples role among identity, attribute and service provider, or consumer.

Identity-Centric Internet

A rich online environment :

- Data exchanges are made between IC-Agent, IC-Agents would be used to exchange personal data or to authorize them.
- An IC-agent is also used to represent the entity on the Web.
- Organizations would use their IC-Agent to realize the access control based on credentials on services.
- Users would employ their IC-Agent to realize access control tasks based on credentials on their personnal data and allow automated multiple access (Delegation).
- IC-Agents allows symmetric relationships between IC-agents (Automated Trust Negociations)

Use cases

Some use cases as a user :

- The IC-Agent is a personal SSO Server.
- The IC-Agent allows users to handle cryptographic credentials usually based on three-tier protocols: Idemix and U-Prove. The IC-Agent has the prover role.

Use cases

Some use cases for users and organizations:

- An IC-Agent helps to manage access control based on credentials.
  - The IC-Agent helps users to handle access control policies requiring multiple credentials to access services.
    - Rent a car if you are of age, you pay, you have a valid driving license, with a discount if you are a student (aggregation of multiple sources of certified personal data).
  - Users can manage the access to online personal data.
    - An organization obtains a credentials from a user's IC-Agent and then use it to retrieve personal data served by the IC-Agent (e.g. online digital records).
    - The user can revoke this access.
    - The personnal data may also be retreived from any attribute provider which trust this IC-Agent for that user. Users have to introduce their IC-Agent to their attribute providers.
  - Access control policies are delivered and interpreted by the IC-Agents.

Use cases

Some use cases for users and organizations:

- Decentralized social network (e.g. foaf)
  - IC-Agents host the personal data and connections with friends.
  - They host the credentials to retrieve personal data from the friends' IC-Agent.
  - A user or an organization just need a viewer plugged to the IC-Agent.

Main functionalities

Overall functionalities of the IC-Agent:

- SSO server.
- Manage requirements of interlocutors (access control policies).
- Manage the credential retrieval (from any sources).
- Manage the presentation of self-asserted and certified data (aggregated).
- (User-managed) Access control on (personal) data.
- Manage trust in interlocutors (authentication, privacy policies, reputation systems, handle trust brokers).
- The whole manageable with a unique dashboard.

Outline

Discovery problem

Let's take the example of the discovery issue with a SSO server.

- In usual federation, the SP lists the IdP (SSO server) or a unique server display the IdP list to the users (WAYF).
- For a public web SSO system, no SP is able to list all SSO servers, especially because even the user may set up her own SSO server, then :
  - The users may indicate the location to the service providers (like with OpenID)
  - The web browser side is "enhanced" to indicate automatically this location to the SP (no standard exists), that could be on the same terminal (e.g. Cardspace)
  - The web browser side is "enhanced" to make the SSO, e.g. the browser wallet (the Web browser becomes the IC-Agent assuming IM functionalities)
  - The SSO system could be inline to handle (and hide) authentication requests (e.g. The IC-Agent may be an http proxy)

Discovery problem

- The issue is the same each time the IC-Agent has not been discovered yet and a service requires it.
- For instance, to handle an access control policy provided by a service provider.
- "The policy must reach the IC-Agent."
- It is necessary to solve the problem one time per session.
- With the IC-agent, whatever the service is, the same location is provided (e.g. an OpenID).

Hosting problem

- The IC-Agent, as any SSO server, can impersonate.
  - It is not worse than if you use the same couple login/password on many SP (impersonation by SP).
  - Efforts are concentrated on the authentication to the SSO server.
- To retrieve credentials, or grant accesses to attributes, the IC-Agent has access to attributes.
- The IC-Agent is the hub of all the personal data exchanges and log them for the benefit of the user control.

Hosting problem

Who hosts users' IC-Agents?

- A state organization? User's university? User's employer? It seems difficult...
- Trust a big society? Why not. (I am not sure that I will).
- A smart phone or a set-top box? Are they under the user control or the control of the telco... but why not.
- Trust another society? Why not.

Outline

Why this could happen.

- We need to provide users with tools to better manage and control the exchange and storage of personal data.
- We need to provide users with tools for a better user experience, for the login and for the handling of the many coming digital credentials: driving licenses, etc.
- We expect that the user side be able to perform identity management operations between a credential issuing and the credential presentation : analyze policies, select sources, select attributes, perform cryptographic operations, etc.
- The users want some means of control. We want to provide them with logs and to make them able to monitor data exchanges when necessary.

Why this could happen.

- Some people hope decentralized social networks.
  - A user may decide to make a data unavailable instead of searching where it is displayed ant try to delete it (“to be forgotten”, even if we know that we can not definitely remove a data revealed).

Why this could happen.

- Famous initiatives
  - OpenID was made for making users have their personal SSO Server.
  - Cardspace addresses a part of these functionalities, but makes the user side heavier (Non standard Web browser + Identity Selector). Only on Windows. Digital Me by Novell is not really achieved on Linux.
  - Higgins made a mock-up with an online Identity Selector, we are quite close to the IC-Agent but authorization management is not handled.
  - Many implementations, mocks-up and research project prototypes (Prime, TAS3) address some functionalities of an IC-Agent.

Outline

Personal SSO Server

The users say which (where) is their SSO Server, no trust needed between the SSO server and the SP.

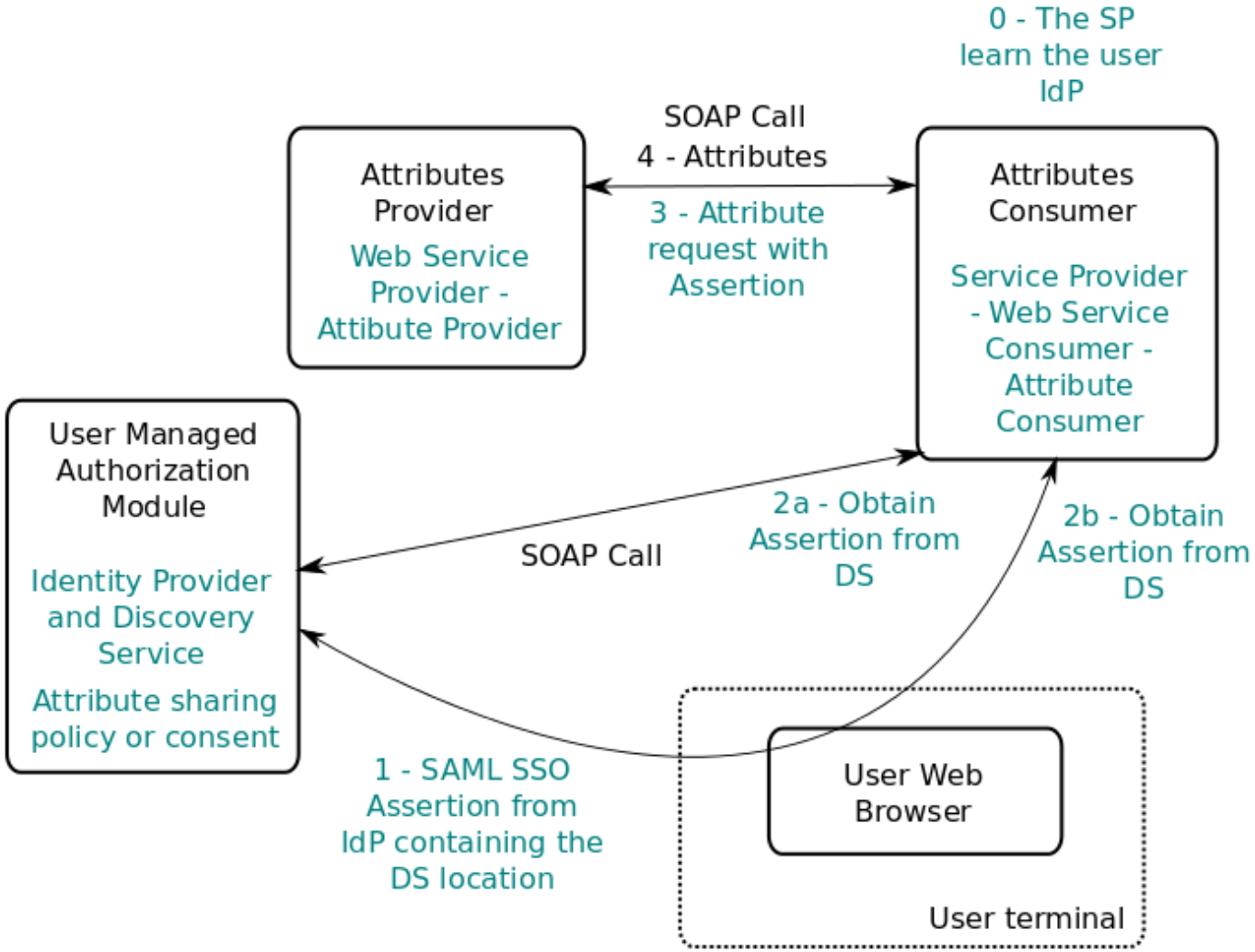
- OpenID
- SAML2 with a way for users to declare their SSO server (or IdP Initiated) and with an “auto-federation” (metadata retrieved from a Well-Known Location) between the SP and the IdP.

We can consider that for a personal SSO server on the Web, OpenID is the bast candidate. Very few public service providers support SAML. No standard way to make the users indicate the IdP location to the SP.

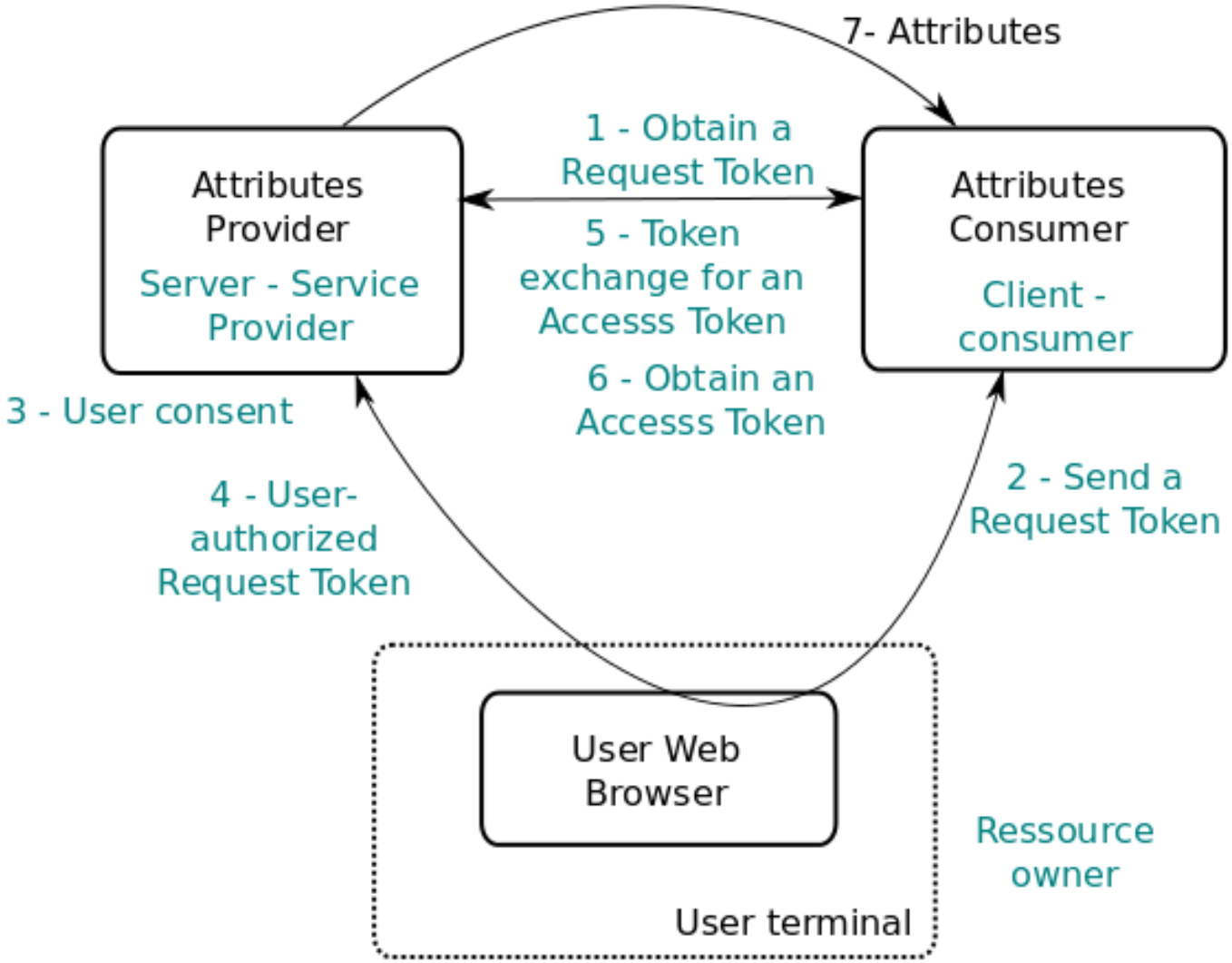
Attribute dissemination and access control

Main candidate protocols.

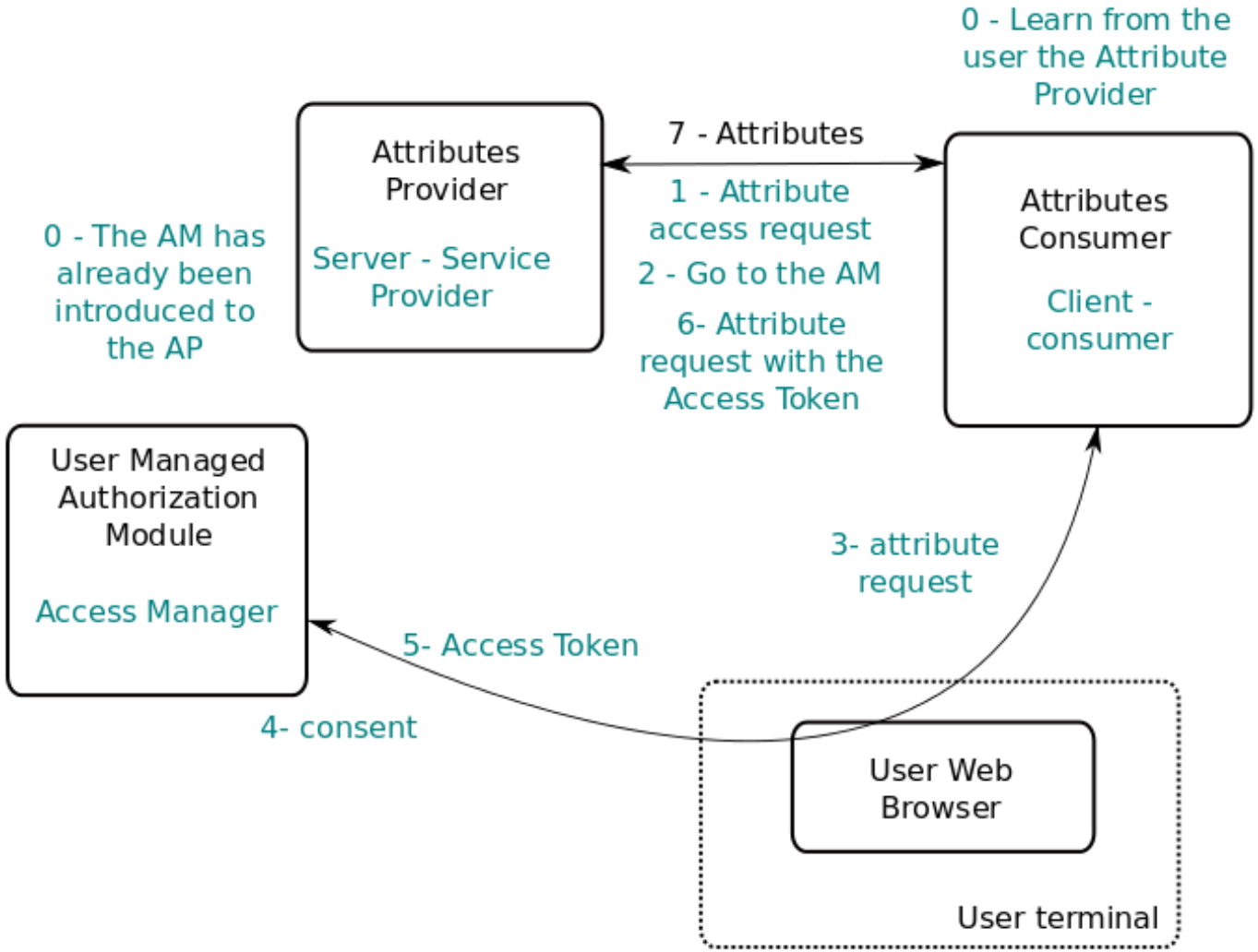
ID-WSF2.0 (SAML 2.0)



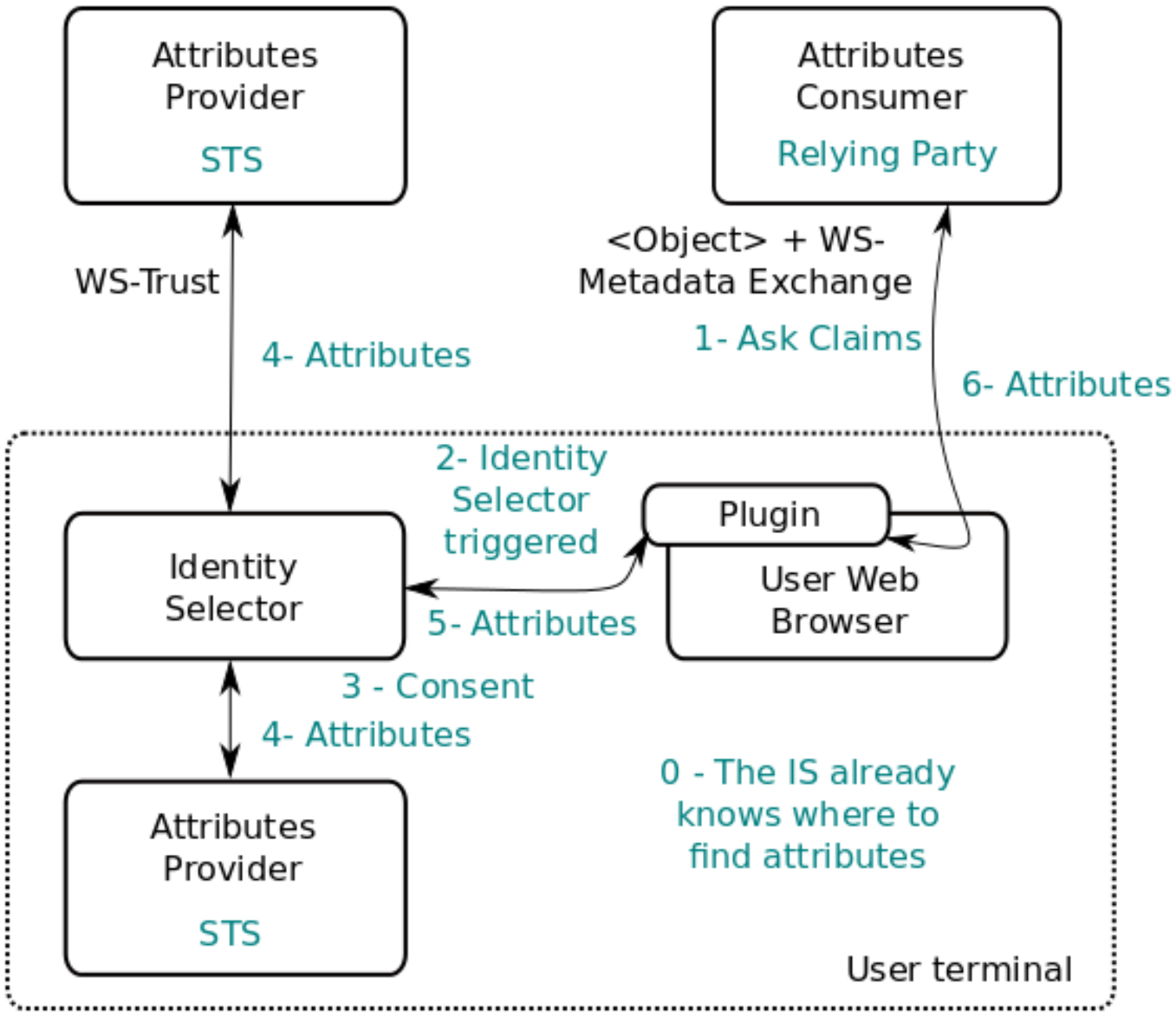
OAUTH 1.0


7- Attributes
1 - Obtain a Request Token
Attributes Provider
Server - Service Provider
Attributes Consumer
Client - consumer
5 - Token exchange for an Accesss Token
6 - Obtain an Accesss Token
3 - User consent
4 - User-authorized Request Token
2 - Send a Request Token
User Web Browser
Ressource owner
User terminal

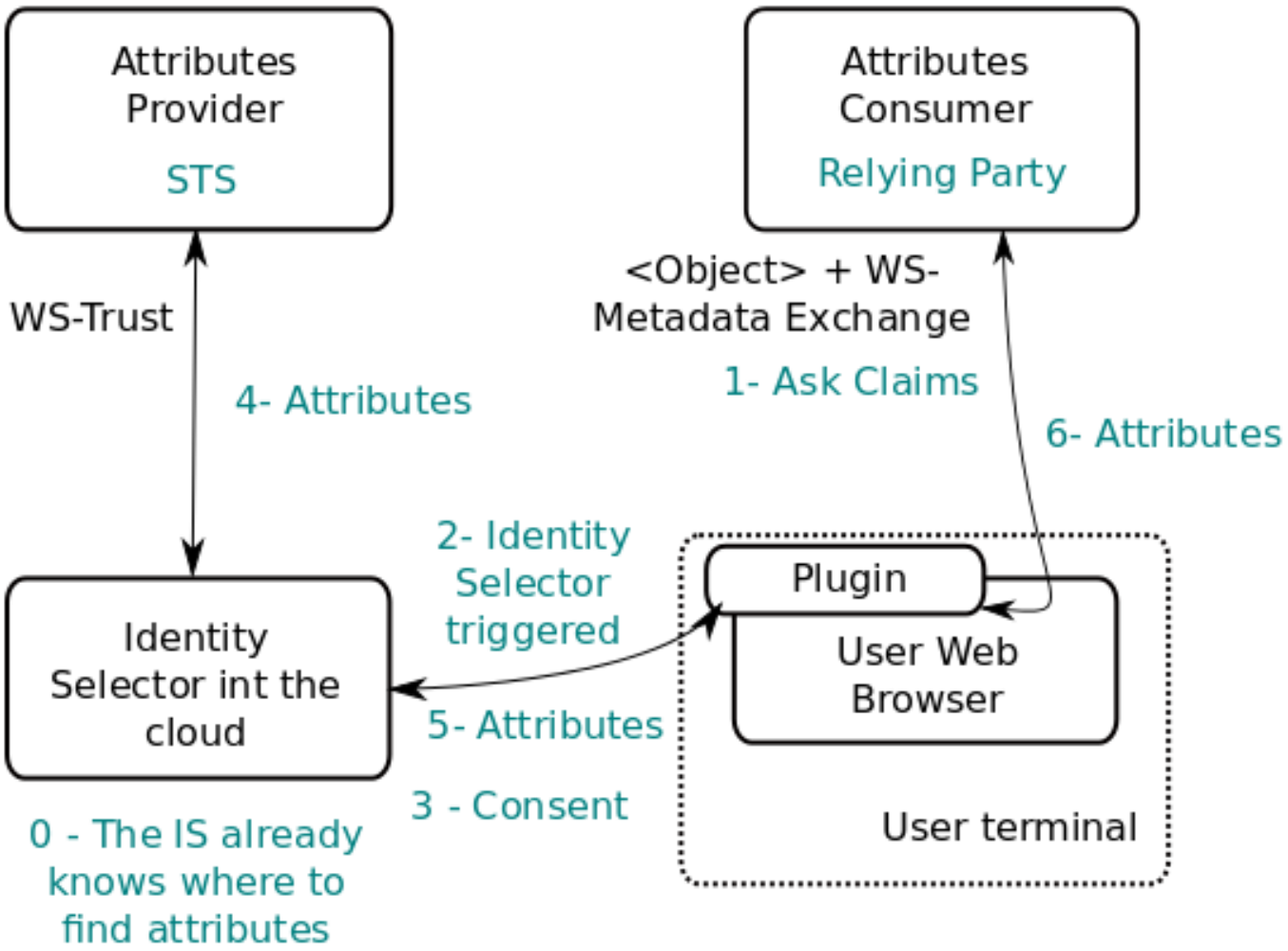
UMA using OAUTH as mush as possible (OAUTH 2.0)



InfoCard


Attributes Provider
STS
Attributes Consumer
Relying Party
WS-Trust
4- Attributes
<Object> + WS-Metadata Exchange
1- Ask Claims
6- Attributes
2- Identity Selector triggered
Plugin
Identity Selector
User Web Browser
5- Attributes
3 - Consent
4- Attributes
0 - The IS already knows where to find attributes
Attributes Provider
STS
User terminal

InfoCard in the Cloud



Outline

Identity-Hub

- We do not propose an online complete IC-Agent.
- For now, very basic functionalities (we are currently setting up the project).
- It is a public service accessible and usable by anybody.
- Little by little we will go towards the IC-Agent
- But now, it is not realistic to set-up the whole functionalities whereas for instance there isn't a widely accepted standard yet for attribute exchanges.

Anyway, who is Entr'ouvert to pretend to such a responsibility?

- Specialized in identity management.
- Only free software (GNU GPL)
- We lead the new Kantara Group dedicated to open source OSSIWG (Join Us Now!) (Officially created the previous week.).

Which softs are used (and developed by Entr'ouvert)?

- Lasso: C implementation of SAML2, ID-FF1.2 and IDWSF2. Bindings for python, perl, php, java. Certified conformant by the Liberty Alliance.
- Lasso mainly depends on openssl, libxml2 and libxmlsec1
- Authentic2 : SAML2 IdP and SP, OpenID provider and RP, CAS Provider, local authentication mechanisms: password, OTP, X509.
- Authentic2 written in Python depends on Lasso, django, django-authopenid.

Identity-Hub Beta version

- www.identity-hub.com
- Functionalities:
  - Personal SSO server as an OpenID provider : your_identifier.identity-hub.com or www.identity-hub.net/openid/your_identifier
  - Multiple authentication mechanisms (The ones of Authentic2).
  - Can be used as a SAML2 IdP, not useful except if you have a SP to test.
  - Identity-Hub is a SAML2 SP and can make the bridge between SAML and OpenID. You can extend the SSO experience between existing federations and your personal RPs.

Identity-Hub Beta version

Coming soon:

- Provide users with directed mail addresses and make Identity-Hub a remailer. Useful to help users to protect their mailbox from spam.

What next?

- Attribute provider and authorization center (Control the dissemination of the certified and self-asserted data).
  - We wait a bit that a standard emerge (OAUTH 2.0, UMA works).
  - We could do it now from SAML2 and IDWSF2. ID-WSF is well-profiled but is not widely adopted. Few implementations (Lasso, ZXID and proprietary softs).
- (Small) Secure store : Very few space to address the case where some documents (e.g. signed PDF) may be given with an attribute retrieval protocol.
- Implement a decentralized social network.

Outline

Accept Identity-Hub

- You have a SAML2 IdP (SSO server)?
  - You may let the user choose where she wants to extend her session.
  - Integrate Identity-Hub as a SP in your federation, it is a real service provider.
    - Our metadata: www.identity-hub.com/authsaml2/metadata.
  - You can already test the bridge SAML/OpenID with the test federation of the French universities.

Accept Identity-Hub

- You are an Attribute Provider?
  - Consider that the attributes are the users' property. If they want to diffuse them, you should accept to diffuse them to anybody the user choose.
  - Some SP may offer discounts to students. Students should be able to retrieve assertions from the IdP of their university (containing only the attribute "student") to prove that they are students.
  - The decision to Trust is for the SP that trusts the universities.
  - In an open environment, the AP should not restrict the SP audience and in any case cannot register (evaluate, trust, etc.) and display to users all the SP.
- Identity-hub behaving as a SAML SP, we can already use the SAML protocol to make the user retrieve SAML assertions. When the user successfully login on the IdP, it should be able to select attributes she wants to send to a SP. Then, Identity-Hub would bridge the protocols.

What to retain?

- You can try Identity-Hub now (Beta).
- You may accept to register Identity-Hub in your federation.
- Join Kantara Groups, especially the Open Source Support Initiative Work Group (OSSIWG), registration will begin in few days.