Mobile agents and their ontology serving a federated identity platform

Farah Layouni and Yann Pollet
Laboratoire CEDRIC
Conservatoire National des Arts et Métiers
Paris, France
farah.layouni@cnam.fr, pollet@cnam.fr

***Abstract*—Like the Web services, federated identity wins gradually businesses. The creation of an infrastructure of federated identity is a viable alternative to current systems. For employees or users, a federated identity leads to a better experience of the Internet, a greater level of customization, more security and a real control of this identity. In this work we will propose choreography for a platform of federated identity based on mobile agents whose benefits will offer more autonomy and flexibility. The use of agents will be accompanied by a definition of ontology allowing them to rely on a single vocabulary, a structured description to better operate and cooperate.**

***Index Terms*—Mobile Agent, Federated identity, Circle of trust, Identity provider, Service provider, Ontology, OWL**

I. Introduction

The identity federation aims to facilitate the sharing of digital assets between institutions and organisations by connecting their authentication services. It becomes possible to open access to digital resources (business application, scientific, educational service, etc.) for an identified population without having to manage local registration of users. The federated identity has a high impact on information systems and several points of vigilance must be observed: we must start by services expected by the user and not by the technical solution; we should carefully identify the partners and the proposed services. Having regard to these requirements for the implementation, these concepts remain potentials values to develop. Indeed, the applications based on federated identity are not unanimous in the public sphere. Local communities and administrations do not mutualize data for the moment. Information systems would exceed the boundaries that still mark the national and local "administrative chain". And this is one of the main objectives of the project FC^2. Eighteen companies are mobilizing around this project (Gemalto, Amadeus, Atos Worldline, CEV Group, Cnam, Constructive Card, Dictao, EADS, Ensi Caen, Entrouvert, Ephi Formation, GIE-CB, INT Evry, Leirios, nCryptone, NTX Research, France Telecom RD, Sagem). The aim of this project FC^2 (Federation of Circles of Trust) is to create architectures, infrastructure and technology platforms for the development of new services based on transparent management and federated identities, both in the field governmental applications that electronic commerce. It is intended to define an overall architecture of identity federation. It will be based on 4 types of architecture: OpenID, CardSpace[1], Liberty Alliance[2] and Higgins[3].

Through this work, we will seek to propose a new choreography for information systems taking advantage of similarities between these previous solutions and allowing a dynamic cooperation between multiple, independent and heterogeneous information systems, with different levels of involvement. The implementation of such architectures required several exchanges of requests and responses which can be costly in terms of traffic data. So the mobile agents[4] intervene to solve these problems. They offer the advantage of reducing the network load, to move the code to the data, to provide more fault tolerance...

This paper is structured as follows. Sec. 2 exposes our architecture . Sec. 3 describes the proposed ontology. Sec. 4 presents our conclusions and perspectives for future work.

II. Execution model

In order to design and develop an execution model for the distributed queries of federated identity architecture, it is more appropriate to introduce, first, the various components of the architecture.

A. Major components

Architecturally, the various solutions of federated identities regroup two fundamental elements:

Identity provider, IdP: It manages the numeric identity of a set of users (creation, deletion, maintenance of their identifying information). IdP offers an authentification service to its users, allowing them to authenticate on the network. When a user wants to reach a service offered within the federation, he uses the authentification service of his attachment institution. Also the IdP can define the users attributes that it auto-authorizes the propagation to service provider.

Service provider, SP: represents the applications that require authentification, thus consuming metadata of users. These metadata is a structured set of data used to describe

the user. They are descriptive metadata and management metadata. They can be held by one or more identity providers. In case of several identity providers, a protocol such as OAI (OAI-PMH = Open Archives Initiative Protocol for Metadata Harvesting)[5] centralizes metadata leaving them to their original location. So the attributes remain divided and accessible.

It is possible that the same organisation plays the role of an IdP in a context and an SP in another. IdP and SP, each deploys interoperable technical solutions for exchanging assertions authentication and attributes. Thus, the two partners are establishing a relationship of trust. The IdP ensures that the attributes of its users are used only for legitimate needs. Conversely, the SP trusts the IdP, especially on realised authentication and the quality of disseminated attributes. The trust stood by commitments of the two providers. This creates "circles of trust" like illustrated in the following figure:

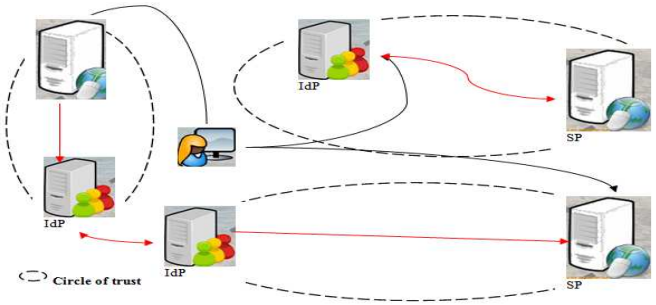

Figure 1. Major components of the platform

This grouping of providers (IdPs and SPs) defines a common set of commitments ensuring a minimum level of trust.

B. Proposed Choreography

We have to note that we have used a specific authentification technique. It is based on the principle of asymmetric encryption. The asymmetric encryption relies on a couple of keys, a public key and a private key, but in our case it will be two private keys that IdP will generate for each user. One will be send to the user, that we note "Cu" and the IdP will keep the other, noted "Cp". Any message to be encrypted by Cu can be decrypted by Cp and reciproquely. In our model, this is the user's query that would be encoded as explains the following scheme:

So, if a user decides to use an application provided by a SP, his request must be encrypted with his Cu then headed to this provider.

In the following, we explain the interaction between different actors in this system under different scenarios.

1) Service Provider and identity provider in the same circle of trust: In the first case, we suppose that the IdP and SP are part of the same circle:

1) The browser or user application sends a mobile agent whose message reflected an encrypted request (with the Cu) to the service provider,

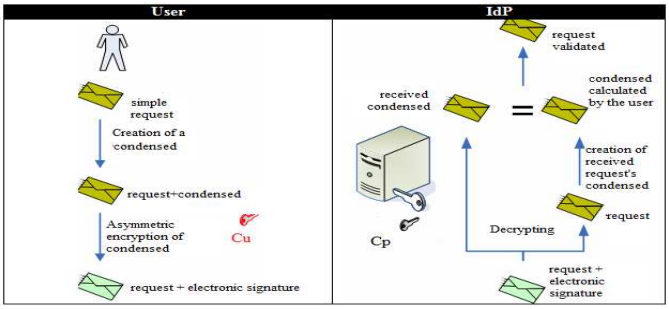

Figure 2. Encryption technique

2) The service provider, without authentication information and unable to decrypt the request, will redirect it to the IdP which is located in the same circle, and he will specify the list of attributes he needs to control access and grant access to resources for the specific user,

3) The IdP will decrypt the request using the Cp associated with the Cu of this user, so it ensures the user's identity. Then he sends the users attributes demanded by the service provider,

4) Having received the decrypted request and the necessary attributes, the SP will execute the query and returns the result to user.

In previous architectures, the user should establish a session with the IdP to ensure its authentication. In our scenario, we combine authentication with request sending through the mechanism of encryption, like noted in the following figure.

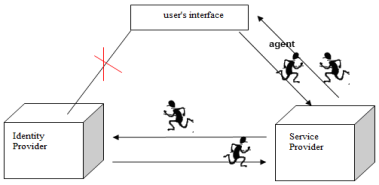

Figure 3. SP and IdP on the same circle of trust

We also optimize exchange between the SP and IdP since the confirmation of authentication and attribute propagation are in one exchange. During the first exchange, the SP remembers that the user has been authenticated. In this way, no encryption or redirection to IdP will be required for next requests.

2) Interaction between different circles of trust: We are in the case where the SP is available for users attached to different circles. The problem that arises is that the SP does not know how to redirect agent transporting request, he did not know which IdP he has to ask to identify the user. This trouble can be solved in different ways, for example, we can use a discovery service like a WAYF (Where Are You From): central component in previous federated architecture allowing user to select his own identity provider. Other way consists on cloning agents and directing them to each existing IdP, also

agents can collaborate to facilitate the location of IdP.

First request to the SP without agents collaboration: To locate the IdP to which the user refers, we will use one of the properties of mobile agents namely "cloning": its ability to copy itself and multiply in the network via a cloning operation. The first IdP which will decrypt the request and send back a response to the SP will be the server in the charge of the identity of this user.

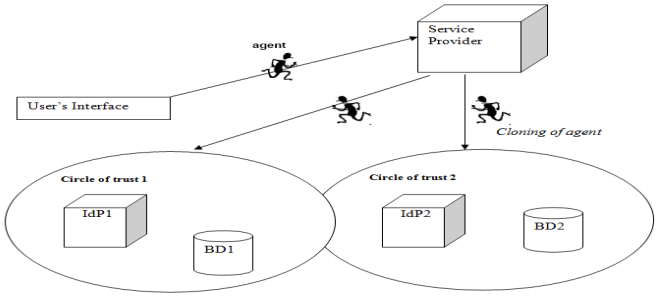

Figure 4. SP and IdP on different circle of trust

It is certainly impressive to have a significant number of agents generated on the network. To overcome this disadvantage, we can organize the circles of trust by neighbourly relations and choose an average number of neighbours to contact. Many studies[6] were performed to estimate the average number, for our case, we estimate it to three, this is linked to the number of the main circles of trust in our platform which will be enumerated later. A user has at least one account in one of these three basic circles.

First request to the SP with agents' collaboration: Agents can cooperate with each other and exchange data, which facilitates and shortens the localisation of IdP. In our case an agent can guide another in locating the IdP attached to the user. This exchange of information is based on user ID. An agent can guide another agent if their both user IDs are in the same range. We assume that the user identifier is composed of two parts: ID-IdP + a random number.

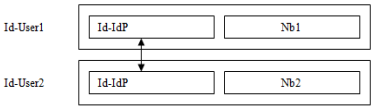

Figure 5. Comparison of ID-IdP

So as illustrated by the previous figure, if two agents succeed in matching their Id-IdPs, they can exchange the location of the IdP, which is very probable to occure because usually IdP manages an important number of users. So the agent can often meet another agent who has already appealed to the IdP it seeks. This collabo-ration will considerably reduce the number of clones. Cooperation may also be extended by combining trace visitation and neighbourliness relations. When visiting a site, an agent may find or submit information in the memory space of the site, for example couples (pre-Id, target direction).

3) Attribute divided among several circles of trust: The use of WAYF will greatly facilitate this task since the user can choose not only an IdP but rather a set of identity servers with which the agent has to communicate in order to collect the different attributes of the user. Also the system allows the user to enter one or more data sources by specifying a plan, a sequence of displacement to guide agent between the various components.

To resume, all exchanges will be conveyed via the agent's body who offers a great value and a high level of security for exchanges. Indeed, the number of queries and answers will be at least halved in comparison with other architectures of federated identities. Traditionally, other exchanges required before four pairs of requests and answers: the first pair between the user and SP for sending the request, the second pair between SP and IdP to ask for users' authentication, a third exchange between user and IdP for authentication and then a fourth exchange between SP and IdP for the spread of attributes. So the introduction of agent will minimise the first two pairs of exchanges by removing the opening session between the user and IdP since authentification information will be conveyed at the beginning with the request. Also the exchange between IdP and SP about sending attributes is eliminated since IdP will transmit it directly by the agent which will confirm authentification. Moreover, this platform will take advantage of agents' properties: portability will help them to better function in a heterogeneous environment, autonomy will foster collaboration between agents and help to a better localisation of the IdP and finally the encryption of the body of the agent offers a higher level of reliability.

A large part of the proposed choreography is based on the collaboration of agents. But this collaboration can not take place if agents don't share the same vocabulary, the same syntax. In the following part, we describe the ontology necessary to our agents who need content interpretable in a unique way by all components of federated identity.

III. Proposed Ontology

In identity federation, the combination of multi-agents with the declarative knowledge, leading to the use of ontologies, is relevant to the development of our architecture.

This combination is justified firstly because of the classic benefits of declarative solutions reporting on the procedural. The declarative solutions provide a more integrated approach with an ontological more direct translation of knowledge domain. With this declarativity of knowledge, changes and evolutivity can be easily taken into account, without recompiling code or stopping execution and this constitutes a significant advantage of scalability.

A. Step 1

The first step consists in defining the domain and scope of ontology, this is facilitated by the answers to some basic questions:

What is the domain that the ontology will cover?
For what we are going to use the ontology?
For what types of questions the information in the ontology should provide answers?
Who will use and maintain the ontology?

In our case the individual is the cornerstone of our domain, we will also join its attributes and its authentication information. Our ontology is intended to cover all elements that surround him from near or far in the context of using a shared informatics service. Many questions may concern him, hence the purpose of this ontology which seeks to demarcate, build a framework for this sphere and especially help share these concepts by a federated identity community. Among these questions, we can include the following:

What are the users? Employees, trainees, providers services, partners, customers, any individual seeking computer service proposed by the federated identity community, an inter-partners application.

Who is behind the identity of users? Human Resources, Management Skills, General Services, ISD. This will be modelled by the identity provider of the circle of trust to which the user belong. The IdP will take charge this identity.

How the lifecycle of user identity is it managed? Creation, modification, deletion...

How are managed the user authorization? It is the service provider who verifies these authorizations after receiving the user attributes.

What are the identities strictly Internal and External? The user can have an identity within its organization called "internal identity", and must also acquire another external identity to share with other partners contributing to provide the service.

How to integrate this platform? The company to which belongs the user must open its information system to strangers in order to take advantage of the many external applications to which its users can access (hosted applications, partners applications,...).

Who will use the ontology? Any organization wishing to improve the experience of its users beyond its information system by extending the authentication mechanism.

B. Step 2

The second step verifies existing ontologies for possible reuse of these ontologies. Many previous works on ontologies [7] propose reusable frameworks, we can cite assembly, extension and alignment of ontologies, by establishing links between the concepts. The existing ontologies will persist and will be part of the new ontology. In most existing public ontologies, we have not found one that can contribute to that we want to create. While many refer to a person as the Aristotle's ontology, but none deal the socio-organizational aspect as we hope, hence the contribution of this work.

C. Step 3

This step consists of making a list of important terms, more precisely capture the words related to the domain and precise theirs senses.

In our case we are dealing primarily with three circles of trust, namely "public circle of trust", "bank circle of trust", "telecom circle of trust". This will facilitate our work to list all the concepts relating to our domain by classifying them according to these three circles:

Public circle: we will find the data identifying a person: name, date of birth, place of birth, country, nationality, sex, address, number of the piece identity, telephone, function...

Bank circle: we distinguish two types of data, those relating to the user as the number of his credit card, her expiration date,... but also data relating to the bank as its identifier, address.

Telecom circle: is the most important sphere in our domain, it includes communication on the network, the communication techniques between the different circles. The following figure illustrates the interconnection of the three circles:

Figure 6. Interconnection of the three circles

Each circle represents a significant number of concepts, functionalities, but since the functionalities of our system do not have the same values and have different objectives, it is interesting to make an abstract sort. To do this we propose a design based on two layers of abstraction:

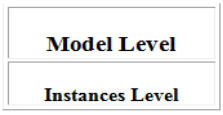

Figure 7. abstraction layers

These layers of abstraction reduce the complexity associated to interconnecting open systems.

-The first layer will define the elements unchanged or immutable referenced to our context.

-A second layer will provide more specifications by adding details concerning variable elements of the platform or a particular instantiation.

When the system is defined, it positions itself in a specific environment. The actors, objects and static interactions of

the system will be placed in the first layer of the model. Moreover, the overall vision provided by this layer is meant to be described by our ontology in a unified context. Thus our developments will obey the same internal logic, logic which will ensure an automated, stereotyped augmentability of the system. This architecture allows a very good separation of layers and makes it easy to add or change components. Let's enumerate elements that will be part of each layer:

The more abstract layer whose data are invariably and identically printed:
Among actors, we name:

- User (Employees, interns, service providers, partners, customers ...) is any individual who needs to use the service of the federated identities to run an application. These users are associated with roles. These roles define a hierarchy of user profiles that are attached various rights of access to functionalities of the system.

- Servers :

Identity Provider, IdP: It manages the numeric identity of a set of users (creation, deletion, maintenance of their identifying information). IdP offers an authentification service to its users, allowing them to authenticate on the network. When a user wants to reach a service offered within the federation, he uses the authentification service of his attachment institution. Also the IdP can define the users attributes that it auto-authorizes the propagation to service provider.

Service provider, SP: represents the applications that require authentification, thus consuming meta-data of users. These metadata is a structured set of data used to describe the user. They are descriptive metadata and management metadata. They can be held by one or more identity providers.

Application server: is a program that provides services to external users.

- Organization: can be an identity provider, a service provider, or both. An identity provider is an organization that issues and manages identities. A service provider provides and controls access to resources of its kind databases and files. Most organisations combine the two: they provide resources to their partner organizations and issue and manage accounts for their own employees.

- Services: these are electronic services based on transparent management and federated identities. These services can be classified into government services (health, interior, e-democracy, public), financial services or telecommunications services. These services will be decrypted in four aspects: a pragmatic, a semantic aspect, a system and a physical aspect.

D. Step 4

This step classifies and hierarchies classes. For this, we will rely on the development process "generalization/ specialization" that we began above. In this way, we create a hierarchy of classes more and more specialized. This has the major advantage of not having to start from scratch when one wants to specialize an existing class. So the super-classes are the concepts of the models layer, so we will have the following classes:

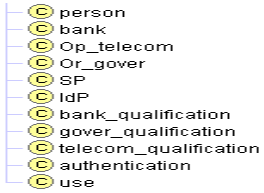

Figure 8. The super-classes

The class "person" is the key of this modelling; it represents the individual who will use the services of the federated identity platform where the SP class represents the application to consume. This person must authenticate hence "IdP" class and "authentication" class which ensures the link between person and IdP. Then we have a class that corresponds to each circle of trust; therefore "bank" class for the banking circle, "Op_telecom" class for the telecom circle and "Or_govern" class for the government circle. And relatively, we will have the "qualification_gover" class involving attributes of a person vis-a-vis his government affiliation, "banking_ qualification" class assemblies bank qualifiers of the person and finally "telecom_qualification" class collects the attributes of the telecommunications sphere.

E. Step 5

This step defines the properties of classes because the hierarchy above does not specify details. So for class "person", we will have the following attributes: Name, address. These attributes will be the only default conveyed by the mobile agent, all those whom we cite after will be exchanged as needed service.

Classes	Attributes
Op_telecom	Operateur_name, coverage, address
Or_gouver	Organisation_name, function, address
Authentication	Login, pwd, fingerprint, signature
Qualification_gover	Date and place of birth, haveFather, haveMother, nationality, family status, haveBrother
Bank_qualification	Credit card number, expiry date
Telecom_qualification	Fixed telephone, mobile phone, subscription duration
SP	URL, service, access control
IdP	ID, Circle membership, Location

Figure 9. classes-attributs

These attributes can have several facets describing the value-type, domain and range of a slot, the cardinalities.

F. Step 6

This step sets restrictions on properties mentioned before. We will describe some whose cardinalities and restrictions

are important in federated identity architecture. The ID of the person must be an attribute with single cardinality to identify the person, locate it and also can be used as key of operations. We choose for this attribute a numeric value. "Circle of trust" is an attribute that can define a circle of trust which helps locating IdP and regrouping organizations belonging to the same circle, it will have a numeric value.
There are various ways of attaching characteristics to the properties, thus greatly refine the quality of arguments related to this property. Among the main features of properties, we find transitivity, symmetry, functionality, the reverse.... In our case this is useful for the following properties: We have specified the asymmetry characteristic for the

```
<owl:ObjectProperty rdf:ID="haveFather">
<rdfs:domain rdf:resource="#Person" />
<rdfs:range rdf:resource="#Person" />
<owl:cardinality rdf:datatype="&xsd;nonNegativeInteger">1</owl:cardinality>
</owl:ObjectProperty>

<owl:ObjectProperty rdf:ID=" haveMother">
<rdfs:domain rdf:resource="#Person" />
<rdfs:range rdf:resource="#Person" />
<owl:cardinality rdf:datatype="&xsd;nonNegativeInteger">1</owl:cardinality>
</owl:ObjectProperty>

<owl:ObjectProperty rdf:ID=" haveBrother">
<rdf:type rdf:resource="&owl;SymmetricProperty" />
<rdfs:domain rdf:resource="#Person" />
<rdfs:range rdf:resource="#Person" />
</owl:ObjectProperty>
```

Figure 10. Properties of family ties

property "haveFather" and also for the property "haveMother" because these are properties operating at one-way, however "haveBrother" must be valid in both directions. The two first properties must have a restriction on cardinalities because a person can have only one father and one mother. We also use transitive characteristic specifically for "Localisation" property which is used to determine the position of the IdP in the platform.

```
<owl:ObjectProperty rdf:ID="location">
  <rdf:type rdf:resource="&owl;TransitiveProperty" />
  <rdfs:domain rdf:resource="&owl;Thing" />
  <rdfs:range rdf:resource="#Region" />
</owl:ObjectProperty>
```

Figure 11. Location Property

Thus we avoid redundancy cases, the relations city->region-> country will be well taken into account. The other attributes have more or less standard values, this is why we are not going to describe them.

This ontology allowed to study the project in three ways: it gave a diachronic view of system: how the structure will evaluate over time under the effect of adding or removing components? A synchronic view, focusing only on elements that characterize it in a precise moment, more precisely in this developing phase of project regardless of what it will become after. And an achronic view where each object has been provisionally separated from organizational procedure.

IV. Conclusion and Future work

In a multi-agent system, the agents communicate between them in order to fullfil the global goal or their local goals. When the system is an open one like a federated identity platform, i.e. the agents enter and leave the system dynamically; the problem of ontology heterogeneity becomes more important and has to be solved. In order to communicate, agents need to share the same ontology (totally or partially) or at least common concepts that are synonyms. Thus, we have created and implemented an ontological model, which addresses the problem of data sharing and interoperability in a federated identity environment. He solved the problem by providing a unified interface for the semantics of data, sharing and reuse of knowledge among information resources that can be dynamic. The formalization of widely shared attributes facilitates interaction and cooperation of mobile agents who seems to be the best solution for nomadic access to distributed information in the platform.

References

[1] K. Cameron and B. Jones, “Design rationale behind the identity meta-system architecture.” White paper, January, 2006.

[2] T. Candia, “Benefits of federated identity to government.” White paper, Liberty Alliance Project, March, 2004.

[3] J. Oltsik, “Services-oriented architecture (soa) and federated identity management (fim).” IBM White paper, November 2006.

[4] F. Layouni and Y. Pollet, “Use of mobile agents in a federated identity structure.” 48th Annual IACIS International conference,Savannah Georgia, USA, september 2008.

[5] S. Oulahal, “Accès unique à des ressources numériques distribuées.” JRES, 2003.

[6] W. Farmer, J. Guttman, and V. Swarup, “Security for mobile agents: Issues and requirements.” In 19th National Information Systems Security Conference, pages 591597, Baltimore, October 1996.

[7] G. Falquet, C. M. Jiang, and JC.Ziswile, “Intégration d’ontologies pour l’accès à une bibliothèque d’hyperlivres virtuels.” 14ème Congrès Francophone AFRIF-AFIA de Reconnaissance des Formes et Intelligence Artificielle, 2004.