Using Infrastructure service orchestration to enable a Federated Identity Architecture

Farah LAYOUNI
Conservatoire national des arts et métiers, Paris France
farah.layouni@cnam.fr

Yann POLLET
Conservatoire national des arts et métiers Paris France
pollet@cnam.fr

Abstract

The aim of this paper is to propose the integration of the orchestration of services within federated identities architecture. The alignment of these two axes of research permits to match homologous subparts existing under federated identities services, helping to resolve them into factors for an optimal reorganization of these services. This orchestration will introduce greater dynamism and scalability in the management of inter-systems and even the integration of new services.

Introduction

Most organizations today require the verification of personal information pertaining to users in order to provide service to users. Privacy of such information is a growing concern and since organizations often ask for similar information, this process can also be redundant and inefficient. Recent proposals dealing with federated identity management have the potential to alleviate such problems. A federation is a set of organizations that establish mutual trust with each other [1]. This allows them to provide a simple and cost effective way to integrate business reservoirs within companies that don't share a common security infrastructure, a typical result of mergers and acquisitions. This significantly reduces the cost of identity infrastructure management by eliminating redundant identity systems or platforms for customer ID management. So Federated Identity standards [2] have emerged in an effort to solve these problems associated with distributed identity data. Primarily, the goal of all federated identity systems is to allow users seamlessly and securely access and make use of systems across domains, without the need to maintain redundant identity data. In order to facilitate this federated identity framework, a circle of trust (CoT) is established between participants. Participants can set up any number of Identity Providers within the circle of trust [3]. An individual is then able to choose which Identity Provider to make use of in order to access services provided by all of the members of the federation. Personal data for the user can be stored in multiple places within the federation, but reduces redundancy by ensuring that pieces of personal data can be linked together and potentially be used throughout the federation. Identity Federation clearly provides numerous benefits both with regard to security and privacy. It also reduces the amount of redundant data stored about individuals and eliminates redundant authentication costs, facilitating better management and updateability.

To implement such paradigms, highly distributed applications are included and implemented in proposed services [4]. They are designed to withstand the rapid changes of applications according to the available and expected services. One of the essential parameters of this flexibility is the weak coupling between services. But our study of these weak coupling services through the project "FC$^{2"1}$ showed that certain types of subservices share many similarities in different use cases. These likenesses are expressed through homologous sub-functions calls like pre-fill form, FAQ or authentication operation. So to continue with the same spirit of elimination of redundancy assured by the federated identity mechanisms, we propose in this article a new organisation, a new architecture of services by combining the common elements that each application can offer.

To reach this objective, the compositions between services are explained in orchestrations functions by using adapted languages that provide different mechanisms to compose and control the invocations between services. These orchestrations are about providing an open, standards-based approach for

connecting federated identity services together to create higher-level business processes. Without a common set

[1] http://www.fc2consortium.org/index.html

of standards, each organization is left to build their own set of proprietary business protocols, leaving little flexibility for true services collaboration.

The first part of this paper proposes a transactional, multi-level process model. Secondly, a specific case study will be explored in order to give a more concrete example of how this solution works. Then we propose a partial solution to a communication protocol for this model. The paper will conclude with a look at future activities.

2. Generalization federated identity services model

The goal of our work is to extract the similarities that exist between the services offered by our federated identity architecture to make it more modular and reusable. Thus each service will be reduced to its basic, elementary function and all the others functions that contribute to its use and its implementation will be grouped at a higher level in order to be shared by other services. This is achieved by the introduction of orchestration notion which describes how services can interact with each other at the message level, including the business logic and execution order of the interactions. These interactions may span applications and/or organizations, and result in a long-lived.

Our solution is based on three layers:

- Front-line (F-L): home tools for users
  - unified components, multi-channel, multi-media, oriented life events,
  - Development of all forms of self-service, allowing "User customization" ...

- Middle-line(M-L): basic bricks serving multichannel strategy home
  - Common services to all interaction channels with users
  - Components and requirements to ensure standardization and interoperability of information systems
    (repositories, directories, trading systems, CRM...)

- Back-line(B-L): administration business services
  - Legacy systems and information system of public sphere

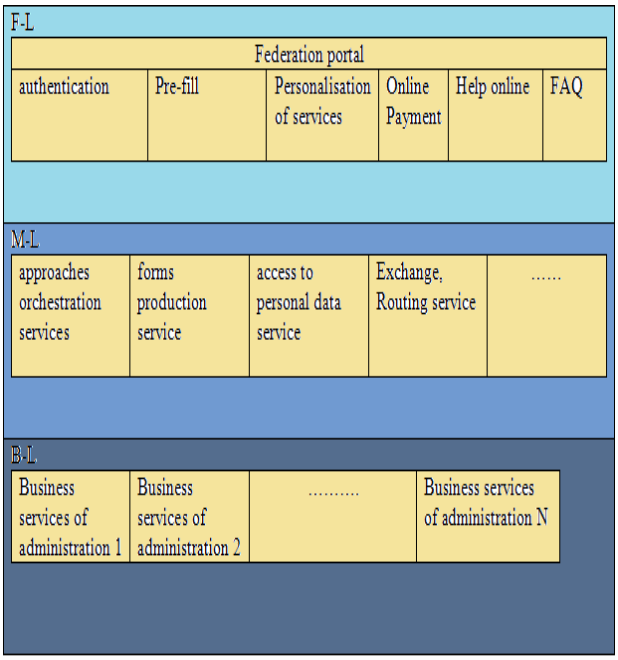

Figure 1. Proposed services model

As well as the previous figure shows, the first level includes all services oriented user: starting by authentication, passing through customization (multilingualism, multichannel), to the online help. The second level forms the intermediate layer between the user and the service itself. The third level offers specific services which are dedicated, by area, depending on the organization of the administration...

So the F-L didn't need to know the business logic implemented by the B-L. It implements process-oriented users, per interaction channel. It is based on services provided by the BO and uses centralized functions. This layer allows a single authentication, pre-fill and storage of personal data. It imposes mechanics of partnership with the administrations to adhere to device.

This orchestration system approaches is the cornerstone of the target architecture of our project. He makes possible the construction of a generic mechanism "oriented users", to respond to any personalized situation. In addition, he proposes modular and

reusable services. This will be better detailed through a use case.

3. Use case and implementation example

3.1 Overview of the functional architecture

Orchestration presented above is only a brick in the architectural structure of our system of identities federation. Indeed our system uses three circles of trust [5]: the government circle, the banking circle and the telecom circle. In each circle there are organizations that provide services. Through our studies, we found that the services proposed are built around an invocation of a hub service specific to each organization, but that requires a framework for implementation [6]. This finding strengthens the proposal outlined in the first section where the service is considered as the building block.

Thus it is at the heart of the frame of each organization we will find the levels described by the previous scheme. In this way, each organization will be fit out as shows the following schema:

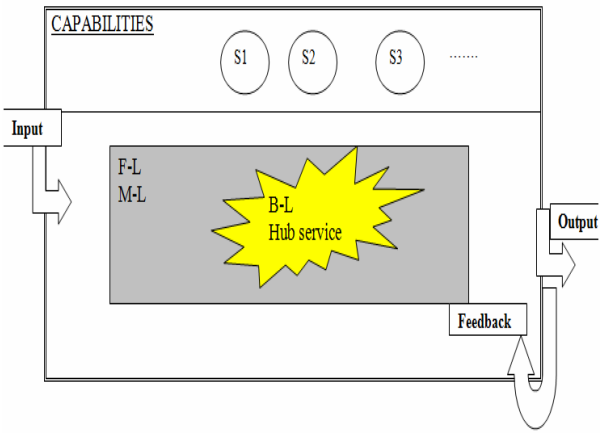

Figure 2. The service process

As part of its accession to the platform of federated identities, each organism has to offer regular services to other organisms demonstrating its collaboration. The implementation of the cooperation services pass through the establishment of a layer detailing aptitudes, capacities of this organization in different domains managed by the federation [7]. Each application has unique needs in terms of sub-services of execution. These needs are obviously different from one application to another, and each organization would be able to interact with other organizations to benefit from the sub-services tailored to their needs. This collaboration and reuse of services presents a considerable gain in terms of resources and time. In addition this orchestration facilitates the collaboration by defining composite services by assembling services. Thus this setting-up emphasizes the needs of weaving between the different organizations.

In a second level, we put the service itself. The functional behavior of this service will be represented as a transformation of the input parameters of service to its output parameters. Furthermore, this principal service will be surrounded by its carrying out decor formed by several functional attributes that specify additional information relating to the service.

We illustrate our approach by the following example. We position ourselves in an information system of a nursery, where a parent look for the registration of his child in a nursery affiliated to the federated identities platform. Usually many papers and documents are required for this service. So it is interested to provide this service online, a real benefit for working parents who do not have enough time to look for different supporting documents.

As illustrated by following figure, the nursery offers the service WS, and Bob wishes to invoke this service WS in order to register his son online. The first step consists of verifying the identity of Bob. The second step concerns the collecting of user attributes. To finalize registration, Bob has to provide at least these papers: proof of address (e.g. EDF invoice), Identification Card for the two parents or family record book, declaration of pregnancy or birth certificate of baby, the two last payslip of the two parents.

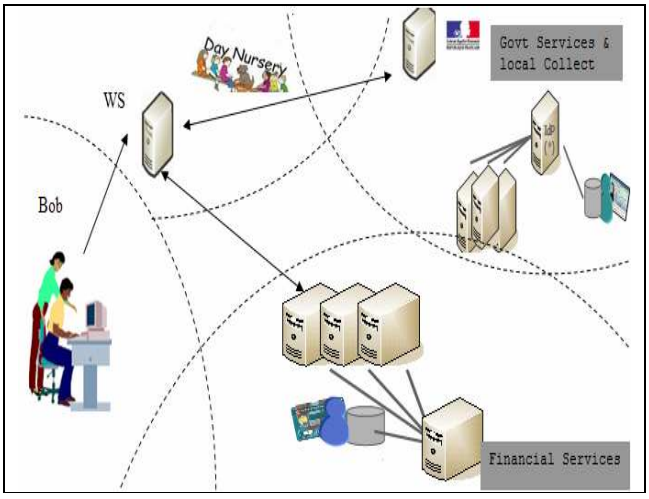

Figure 3. Interaction of the nursery with the other CoT

Like presented by the previous figure, the nursery that provides the service must interact with other systems to ensure the realization of this action.

First, we describe via the next illustration the SI of the nursery and its interactions with other SI:

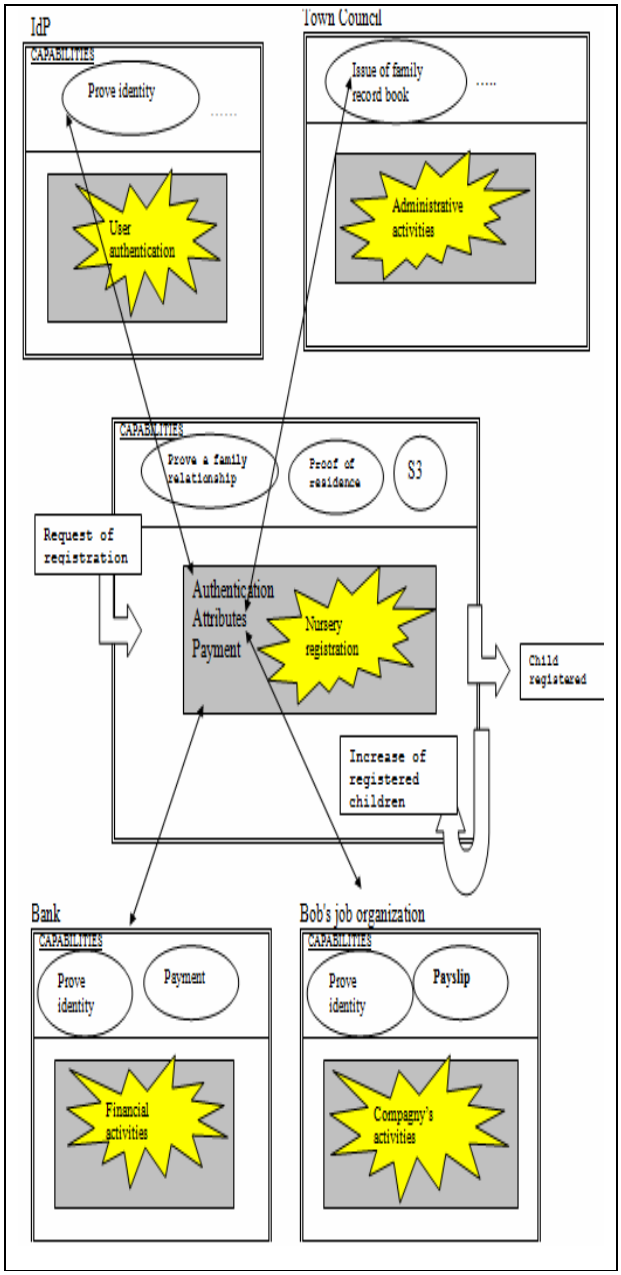

Figure 4. Interaction of the nursery's SI with the other S.I.

The nursery offers mainly the registration service. This service accepts as input the registration form and engenders as output a predicate asserting the inclusion of the child and the modification of the internal system of the nursery because there will be a change in the admission capacity by the inclusion of a new child. But the invocation of the service doesn't come down to a simple implementation. This kind of service as the majority of the services of a federated identity platform pass through a collection of attributes to verify the identity of the user and the information he provides. To do this, the SI of the nursery will take advantage of sub-services offered by different SI of the other circles of trust to replace the presentation of documentary evidence in the case of dematerialized procedure. Indeed, the registration procedure requires for example the provision of documentation such as proof of address. In a paper procedure, presenting a Telecom or electricity bill can fulfill this task, but in the case of a dematerialized procedure, we need to relinquish the physical presentation of these pieces. This application considers that the value of some data is "certified" by an outside entity. Telecom operator may for example provide a "certified address" to do without sending documents. It will be the same for the payslip of the parents, because their company provides a sub-service for issuing payroll. The town council also will facilitate the task of verification of relationship between the citizen and the person concerned by the registration by issuing a certified copy of the family record book. Finally to proceed with online payment, the SI of the nursery will establish a direct link with the citizen's bank to verify the accuracy of communicated parameters of his credit card or other means of payment.

Also, we argue that interaction is an important aspect of study as well as business objects and processes [8]. In fact, interactions allow global, unified and consistent view of business objects and synergy of processes, but also make explicit emergent knowledge, which has considerable added value for the organization. Yet, interactions do not exist naturally. It is necessary to make them explicit and visible all more so since the exploding popularity of the federated identities systems allows building distributed interacting subsystems; and accessing a variety multimedia structured, semi structured or unstructured information representing business objects and processes.

Therefore, communication artifacts are required: (i) to allow global, coherent and transparent views of business objects and efficient distribution of processes, and (ii) to avoid, design of the model each time new SI is introduced.

3.2 Communication protocol between the functional blocks

In the previous sections we list the various components of our model but we were not specific about the means of interaction between different information systems. In this section we seek to enrich the orchestration with a choreography based on mobile agents. To do this we propose multiagent solution coordination, for the choreography of services, in which the capacities of collaboration services are modelled with introspective agents [9]. These agents are able to reason about their own actions (or the services they offer), to dynamically decompose a task according to their skills, and coordinating with other agents to overcome their limitations and needs to cover meet. In our architecture, we propose several organizations that offer sub-services which may be more or less similar. So the choice of which agency to contact or the selection of the most suitable service proved essential for the smooth running of the model.

We start by defining the selection of services. The service selection is the decision to choose services from a particular set of services based on functional requirements or parameters of service quality. Accordingly, in the context of dynamic environments such as the identities federation, where services are changing and the needs of users vary and may not all be planned in advance by an expert, the service discovery should be on the fly and the choreography of these, instead of previously provided through a scheme of composition, must be done in a dynamic function of the needs outlined by the user, the functional and structural characteristics of the services found and interactions resulting from them.

Since mobile agents are known by their autonomy, quality that is absent in the solutions based on web services, we will introduce this concept in our model as illustrated by the following picture.

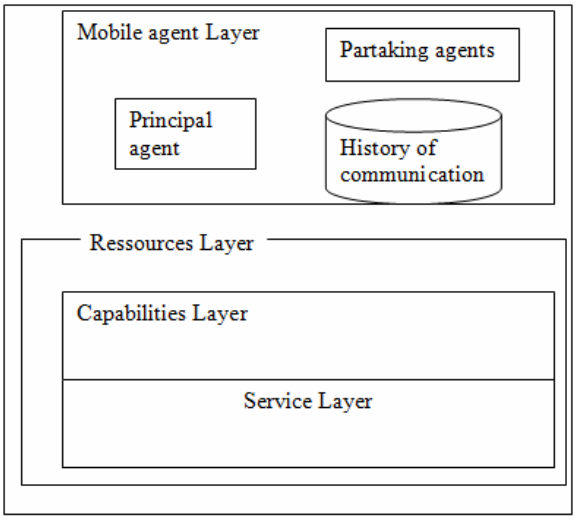

Figure 5. Multi layer federated Service architecture

Therefore each organization providing capacity must be equipped with another layer of communication that will serve as a context for the creation, communication and execution of agents assisting in the achievement of its service. So when an information system needs subcontracted a part of the execution of the service or collect other data information systems, he has to create an agent to discover and locate the service he needs through this federated platform. The discovery service is the search process of the most appropriate service provider, for a given service request. For the moment, we suggest that this discovery is achieved via a broadcast diffusion [10], [11] as the number of circles of trust does not exceed three but we will try in future work to convert this way to a multicast. Thereafter, the system will retain the first received response. Once the candidate service has been discovered, they will interact together by sending one or more agents according to the need of communication. The various operations of reasoning, treatment or construction messages are set entirely at the agents. The interaction of services is therefore governed by agent's layers. We attribute two main roles to agents:

- The principal agent: this agent is the primarily responsible for interacting with the home organization of the service. He distributes its requests to agents involved in coordination. At the end of coordination, he receives responses from agents. He is also in charge of sorting them according to the constraints of the user.

- The partaking agents: their role is to coordinate in order to satisfy all requests from the user.

Mobile agents in our model interact and coordinate in terms of received or previously trade messages. To do this, each agent has a history to back up all phases of exchanges. The history lists all traces of the interactions of agents, including the previous messages, as well as the innovatory message of each interaction. Furthermore, this history can serve for modelling experiences feedback for future operations that will require the same approach.

The inter-system communication is not the main purpose of this article; we describe here a simple approach that allows us to have bricks of formal solution that will rely on Contract Net Protocol [12].

Conclusion

Environments such as federated identity system and multi-systems environments are open and distributed. They are characterized by very flexible and dynamic (where new properties can appear for a service and new services may be available on a daily frequency) services and where needs of users for services vary. In this context, the process of composition of services to meet the needs of the user may adapt dynamically to the needs of the latter with a minimum intervention of his part.

Within this framework, our research operates. After presenting this issue, this paper describes our proposal. This one consisted on the design of a dynamic approach of federated identities orchestration services based on multiagent coordination mechanisms.

But this coordination solution remains informal. So in the future work, we will try to develop a formal ontology, specific to our field. Even, we plan to introduce a QoS vector in the response message transmitted by the mobile agent, to associate with each sub-service a QoS. This will make the choice of subcontracting organization more effective.

References

[1] K. Kang, “Network identity”, Seminar on Networking Business, 2004.

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

[3] N. Dors, “Shibboleth architecture”, JRES, 2005

[4] K. Cameron and B. Jones, “Design rationale behind the identity metasystem architecture”, White paper, January, 2006.

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

[6] F. Layouni and Y. Pollet, “Ontology for mobile agent cooperation in federated identity platform”, ASWC Bangkok Thailand 2008.

[7] J. Oltsik, “Services-oriented architecture (SOA) and federated identity management (FIM).” IBM White paper, November 2006.

[8] C. Batini, M. Lenzirini and. S.B. Navathe, “A Comprehensive Analysis of Methodologies for Database Schemas Integration”, *ACM Computing Surveys*, 322-364, 1986.

[9] S. Lindström and W. Rabinowicz, “Dynamic Doxastic Logic for Introspective Agents”, Erkenntnis, Volume 50, Numbers 2-3, may 1999.

[10] A. Banerjee, S. Bandyopadyay, "Paradigms for Reliable communication Protocols in Mobile Agent Based Systems", In Proceeding 31st Annual Hawaii International Conference on System Science, Vol. 7, 1998.

[11] F. Al-Shrouf, M. Eshtay and K. Abu Humaidan, ”Performance Optimization for Mobile Agent Message Broadcast Model Using V-Agent”, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.8, August 2008

[12] Smith, R.G.: The Contract Net Protocol: High-level Communication and Control in a Distributed Problem Solver. IEEE Trans. On Computers C-29(12): 1104–1113, 1980