Federated Identity Architectures evaluation

Uciel Fragoso-Rodriguez
Instituto Tecnológico Autónomo de México, Mexico
{ uciel@itam.mx}
Maryline Laurent-Maknavicius
CNRS Samovar UMR 5157, GET – Institut National des Télécommunications, France
{ maryline.maknavicius@int-evry.fr}
Jose Incera-Dieguez
Instituto Tecnológico Autónomo de México, Mexico
{ jincera@itam.mx }

1. Introduction

The Internet has brought a huge increase in the number of on-line transactions among individuals and enterprises, accelerating business relationships like B2B (Business to Business), B2C (Business to Client) and B2E (Business to Employee). At the same time, user's requirements have become more complex since they demand faster and more secure accesses, in addition with mobility facilities. Besides, the technological convergence has allowed multiple services and Service Providers (SP) to be integrated in order to offer joint services. In a traditional setting, a digital identity must be assigned to the user by each SP he wants to access. The SP must have an identity management system to handle the identity lifecycle (creation, management, usage and elimination). In this context, users feel uncomfortable handling several digital identities, one from each SP. In addition, users generally have no control on the exhibition of their personal information, which constitutes a privacy problem that in some countries has legal repercussions. To deal with these problems, several Federated Identity Architectures (FIA) initiatives have recently appeared that propose a model of global identity management targeting unification, sharing or linking the digital identities of the users among different domains. Given their novelty, there are very few experiences with regards to the implementation of FIA projects and several open issues have yet to be addressed.

2. Objectives

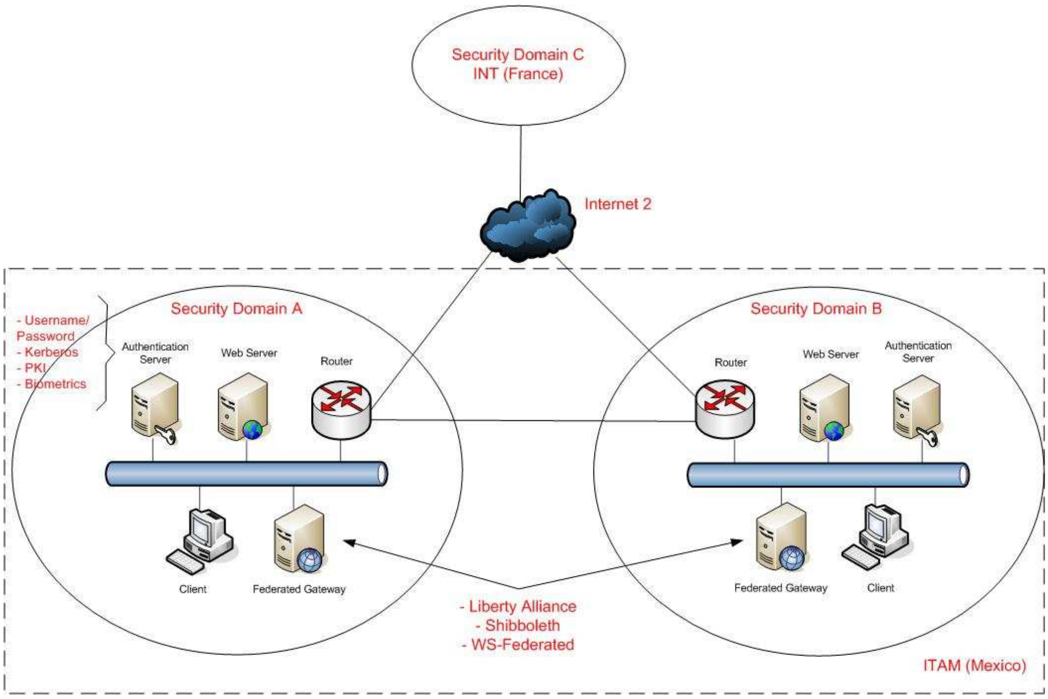
- To establish a set of criteria that must fulfill a model of federated identity management from the point of view of effectiveness, interoperability, privacy and security in a complex context of multiple services and providers.
- To define appropriate metrics for evaluating FIA implementations: security, performance, easy of use, scalability, etc.
- To implement a laboratory test bed in order to evaluate the main current FIA initiatives. The test bed will include implementations in two academic institutions: ITAM in Mexico and INT in France.
- To develop Web applications and Web services that permit to evaluate the interoperability among the different initiatives.
- To identify the main guidelines towards an integrated Federated Policy Management framework.

3. Accomplishments to date

The FIA initiatives under evaluation are:

- Shibboleth.- An academic initiative of University members of Internet 2. Its objective is to facilitate the collaboration and access to protected resources among institutions without using external or temporary accounts. Some applications that could take advantage of this solution are: access to library database information, distance learning courses, collaborative applications for project development, etc.
- Liberty Alliance.- A commercial initiative to establish technological, business and policy framework for implementing a Federated Identity Architecture.
- WS-Federated.- A reference model to provide identity security for Web Services from a technological and business point of view.

The laboratory infrastructure is under implementation with the necessary elements to test these initiatives. Architecture will be individually tested, but they will need common services and at a later stage of the project they will interact. The following diagram shows the logical network topology and components required to carry out the evaluation:



The laboratory has two Security Domains, representing each one a different enterprise or organization. Within the security domain, the following components are present: the *Authentication Server* which contains the user identity information, the *Web Server* which has the web resources to share, the *Router* to make the network connection of the security domain, the *Client* from where the user will access the local or remote web resource, and finally, the *Federated Gateway* which contains the software for the IdP and SP functionalities for each FIA architecture. Up to now, Shibboleth and a commercial product compatible with Liberty Alliance are under implementation. The main functionalities (single sign on, identity federation, attributes exchange, identity privacy and anonymity control, among others) of each implementation will be tested between the Security Domains, locally as well as remotely with INT through Internet 2.

4. Future plans

Once the main functionalities of each initiative have been tested, some modules will be modified or created in order to accomplish the following objectives:

- To get a minimum level of interoperability among the different FIA architectures, considering that in the near future, none of the initiatives will dominate the market.
- To establish an evaluation framework for the proposed metrics like performance and scalability, mainly when these architectures are to be deployed at a large scale.
- To evaluate the degree of secure information exchange, so that the user’s privacy rights may be preserved according to the law compliance that an organization must fulfill.

5. Conclusions

The evaluation of the principal up to date FIA architectures, will allow us to specify the main functionalities and characteristics that a FIA model must fulfill related to a specific application scenario in order to obtain the best cost/benefit relationship.