Federated Identity Architectures

Uciel Fragoso-Rodriguez
Instituto Tecnológico Autónomo de México, México
{uciel@itam.mx}

Maryline Laurent-Maknavicius
CNRS Samovar UMR 5157, GET – Institut National des Télécommunications, France
{maryline.maknavicius@int-evry.fr}

José Incera-Dieguez
Instituto Tecnológico Autónomo de México, México
{jincera@itam.mx}

Abstract

Users and organizations are looking forward to tools that provide the management of digital identities offering a fast and secure way to access computer resources. The problem is to share the digital identity or link it to other identities so that service access is possible through multiple Service Providers (SP). Up to now, several initiatives known as Federated Identity Architecture (FIA) have been proposed for global identity management models. The article describes FIA solutions proposed by academic and industrial organisms (Liberty Alliance, Shibboleth and WS-Federation). It analyzes their main characteristics and presents some remaining issues and challenges.

1. Introduction

The Internet has brought a huge increase in the number of on-line transactions among individuals and enterprises, accelerating the business relationships like B2B (Business to Business), B2C (Business to Client) and B2E (Business to Employee). At the same time, the requirements of the users have become more complex since they demand faster and more secure accesses, additionally with mobility facilities. Similarly, the technological convergence has allowed multiple services and Service Providers (SP) to be integrated in order to offer joint services. For each accessed service, a digital identity must be assigned to the user by the SP, who must have an identity management system to handle the identity lifecycle (creation, use and elimination) [1].

Under this context, users feel uncomfortable handling several digital identities, one for each service. Besides, in most cases, users do not have control on the exhibition of their personal information, which constitutes a privacy problem that in some countries has legal repercussions. From the point of view of the SP, the identity management process represents a very high administrative load in financial and operative terms. Nevertheless, the main challenge faced by SP is the difficulty to integrate with other SPs in order to offer combined services and to handle a unique identity of the user. To deal with this problem, several FIA initiatives have appeared recently. They propose a model of global identity management that allows to unify, to share or to link the digital identities of the users among different domains. After introducing FIA basic elements, three main FIA initiatives are described. For each initiative, its architecture, main components and operations are briefly explained. Finally, a comparison is made in terms of functionalities, and remaining issues and challenges are discussed.

1.1. Digital Identity Elements

Some definitions are first given to understand the main components of a digital identity and the relationship among them [1].

Digital Identity - The electronic representation of an *entity* within a domain of application.

Entity - A person, a group of persons, an organization, a process or even a device, that is, any subject able to make a transaction.

Domain of Application - The application scope where the digital identity has validity, for example: a company, a hospital, a club, a university or the Internet. Note that an *entity* may have several identities within the same domain of application. For instance, a professor could have identities of both professor and student in case he takes continuous education classes.

Identifiers - A digital identity is composed of identifiers or attributes, which can be assigned, selected or they can be implicit to the user. Examples of attributes are: date of birth, address, employee ID, Social Security Number, among others.

Credentials.- Any elements serving to authenticate an identity by means of the validation of its identifiers. A credential can be a password or the answer to a challenge (what he knows), or it may be constructed based on a smart card or a digital certificate (what he has), or any characteristics of the entity as his fingerprint, his eyes or his voice (what he is) . The type of credential used during the authentication process depends on the business security requirements.

Figure 1 shows the existing relationship between the elements that compose a digital identity.

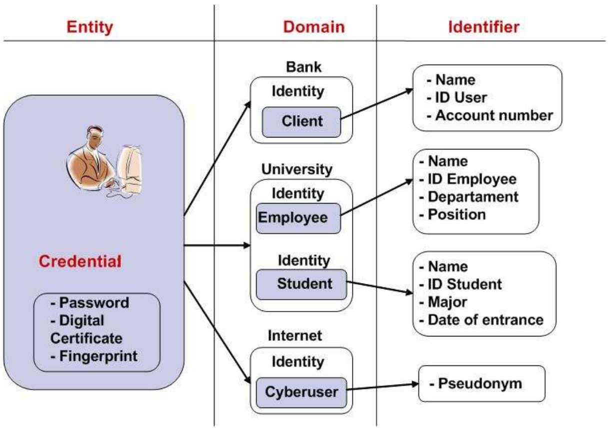

Figure 1. Relationship between the elements of a digital identity

1.2. Identity Management Evolution

Identity Management (IM) refers to the processes that handle the lifecycle of a digital identity, that is, the creation, handling and termination of a digital identity within an application domain. IM also has to deal with the process of authentication, as well as the definition of the access control policy that an organization must fulfill in order to give access to protected resources [2].

Historically, IM systems evolved from islands of identities, where each area of the organization managed in an individual way its identities with no integration. Later on, centralized solutions for unique handling of the users identities were implemented. Today, a number of ready-to-use products are available for organizations to implement their own private centralized solution. Nevertheless, nowadays it is common that users require access to resources that are outside their organization due to the growth of managed services (outsourcing) or business agreements between organizations. This is why the current models of identity management must evolve to a model that supports unifying or linking digital identities in a federated architecture.

1.3. Federated Identity Architecture

A Federated Identity Architecture (FIA) is a group of organizations that have built trust relationships among each other in order to exchange digital identity information in a safe way, preserving the integrity and confidentiality (privacy) of the user personal information [3]. The FIA basically involves Identity Providers (IdP) and Service Providers in a structure of trust by means of secured communication channels and business agreements [4].

IdP manages the identity information of the user and does the authentication process in order to validate his identity. Within a FIA there could be one IdP (centralized model) or several IdPs (distributed model). The centralized model has the advantage that the identity information is not disseminated, facilitating its confidentiality and integrity, but it could represent a bottleneck and a single point of failure. In the distributed model, the authentication process can be done in any IdP, providing flexibility and load balancing. However, this approach requires more complex and secure mechanisms to exchange, and manage the identity information and to guarantee its integrity.

SP provides one or more services to the users within a federation. The enforced access control policy protects the services themselves by granting access only to authorized users. This access control policy is established when the federation is formed.

The FIA must fulfill the following main functionalities from the point of view of users, identity providers and service providers:

Single Sign-On (SSO).- SSO allows users to authenticate with an IdP and then to access services provided by several SPs with no extra authentication.

Attribute exchange.- Once the user is authenticated by the IdP, the SP needs additional attributes to provide personalized services. Thus, the FIA must facilitate attribute exchange between IdP and SP.

Personal information privacy.- Confidentiality and integrity of the user´s personal information must be guaranteed in such a way that the exposure of the identity attributes can be controlled by the user.

Identity lifecycle management.- Whether the model is centralized or distributed, the creation, maintenance and elimination of a digital identity must be simple and must not represent high operational costs.

Standardized architecture.- The FIA must be based on standards for an easy integration of new SPs and IdPs.

In the following sections, the architecture, elements and operations of the three main FIA initiatives, will be briefly described. Finally, they will be compared and their principal challenges will be exposed.

2. Liberty Alliance

Liberty Alliance is a group of more than 200 companies from diverse sectors. It was launched in 2001 with the objective to establish a technological, business and policy framework for implementing a Federated Identity Architecture [5].

The Alliance developed a business guide to help companies converge towards a business agreement and conform to a federated architecture focusing on feasibility, risk, mutual trust and compliance aspects.

2.1. Architecture

Liberty Alliance is a framework that includes a set of technical and business specifications for establishing a Federated Identity Architecture. Its architecture shown in figure 2 includes three modules that operate on technological open standards developed by organisms like OASIS, W3C and IETF[*].

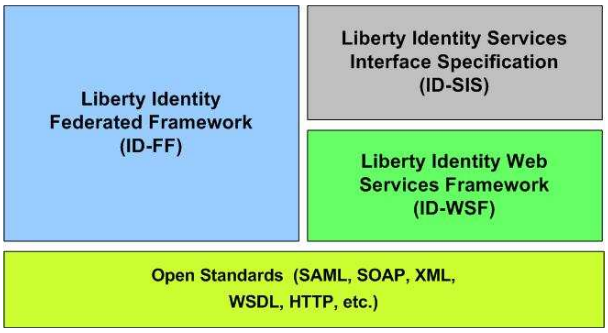
Liberty Identity Federated Framework (ID-FF)
Liberty Identity Services Interface Specification (ID-SIS)
Liberty Identity Web Services Framework (ID-WSF)
Open Standards (SAML, SOAP, XML, WSDL, HTTP, etc.)

Figure 2. Architecture of Liberty Alliance

ID-FF (Identity - Federation Framework) is a set of specifications targeting identities federation and management. This module composes the fundamental part of the architecture, defining a set of functionalities like: account linking (identity federation), session management (Single Sign On and Single Sign Out), affiliation (capacity to select the IdP for identity federation).

ID-WSF (Identity - Web Services Framework) specifies a framework for Web Services in order to create, discover and request identity services. ID-WSF also operates on open protocol standards [6] and supports the following functions: attribute sharing (with possible previous authorization from the user), discovery of services, security mechanisms to transmit messages, etc.

ID-SIS (Identity - Services Interface Specification) serves to build security services of higher level (applicative services) based on the ID-WSF framework. Examples of ID-SIS services include: personal information request, geo-location services, directory services, etc.

2.2. Elements and operation

Liberty Alliance defines a Circle of Trust (CoT) to which SPs and IdPs adhere by signing a business agreement, in order to support secure transactions among CoT members.

As depicted in figure 3, each CoT member might know a user under distinct identities. All identities are related or federated in such a way that the authentication process can be performed by any CoT member. In that sense, Liberty Alliance is said to be distributed because any IdP within the CoT may authenticate a user.

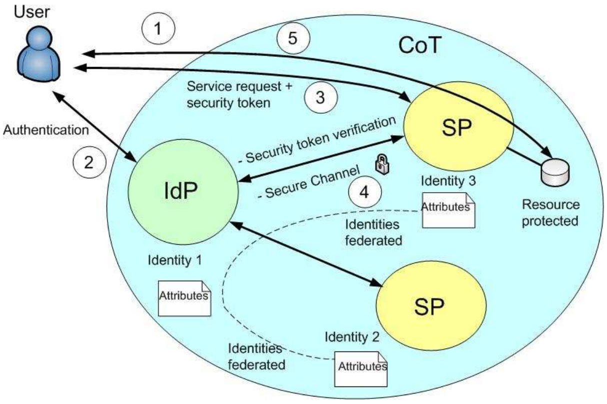

Figure 3. Circle of Trust (CoT)

For the user to access any service inside the CoT (1), the SP asks the user to select an IdP, and the user is redirected to this IdP for authentication (2). The IdP authenticates the user and assigns a “security token” with identity information which is next forwarded to the SP(3); the “security token” is verified between the SP and IdP in a back secured channel (4), and in case of validity, access to the service is granted (5). If the SP

[*] OASIS (Organization for the Advancement of Structured Information Standards), W3C (World Wide Web Consortium), IETF (Internet Engineering Task Force)

requires additional attributes, they are requested to the IdP through the secure channel.

The CoT model demands that SP trusts the IdP, thus, it requires a secure communication infrastructure that guarantees the integrity, confidentiality and non repudiation of the interchanged messages. The incorporated security mechanisms in the specification of Liberty Alliance include security in the communication channels as well as security in message exchanges. The secure communication can be implemented by means of current standard protocols such as TLS, SSL and IPsec. These protocols implement authentication mechanisms between SP, IdP and users before initiating the message exchange [5].

3. Shibboleth

Shibboleth is 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. [7].

In Shibboleth, information relative to the users digital identity is managed by the institution to which they belong. When a user requires access to the resources located in another institution, the identity attributes are sent along with the request but only attributes previously agreed to be shared may be communicated. These attributes are finally used to make decisions of accepting or rejecting user's access request according to the local access control policy. The main interest is to distinguish between users belonging to an institution and students from a specific course. Thus, it is no necessary to send the real identity of the user, and so privacy of personal information may be guaranteed in Shibboleth.

3.1. Architecture

The architecture is also built upon open standards such as: HTTP, XML, SOAP, and SAML [8]. Figure 4 depicts the services composing the architecture.

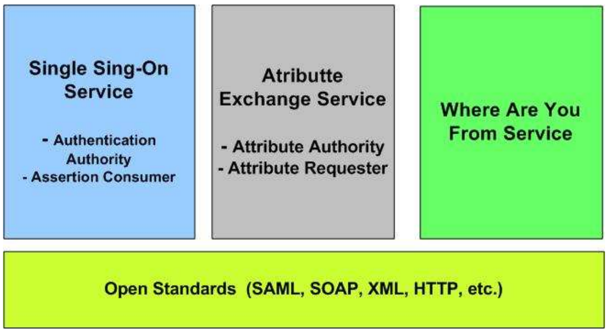
Single Sing-On Service
- Authentication Authority
- Assertion Consumer
Atributte Exchange Service
- Attribute Authority
- Attribute Requester
Where Are You From Service
Open Standards (SAML, SOAP, XML, HTTP, etc.)

Figure 4. Shibboleth architecture

Single Sign-On Service.- SSO initializes the process of authentication. This module does not specify how the user authentication must be done, but it works in coordination with the local authentication system. This service uses two components (Authentication Authority and Assertion Consumer) to exchange authentication assertions in order to generate a security context in which the users can access the protected resources.

Attribute Exchange Service.- This service sends attributes to the SP, who applies the access control policy to determine whether access to protected resources is permitted. Two functionalities are defined to accomplish this service: the Attribute Authority and the Attribute Requester. The attributes are only divulged if the local policy defined by the IdP and the user gives permission, ensuring the personal information privacy.

WAYF (Where Are You From).- WAYF is an optional service that enables the SP to locate the user's IdP of subscription. WAYF is such like a directory that interacts with the user for the selection of the IdP that conducts the authentication operation.

3.2. Elements and operation

Shibboleth consists of three elements: *Origin* (Identity Provider), *Target* (Service Provider) and optionally the WAYF service. The *Origin* maintains users' accounts (credentials and attributes) and carries out the authentication function. In addition, it generates authentication or attribute assertions towards the *Target*. The *Target* manages the protected resources and controls its access based on the identity assertions emitted by the *Origin*. The WAYF service if implemented, allows the user to select the Origin in charge of the authentication process [8]. Figure 5 shows the relationship and operations between Shibboleth components.

When the user needs access to a protected resource located outside his organization (1), the *Target* asks the user to authenticate himself. Usually, the *Origin* or IdP is the organization to which the user belongs, optionally, the WAYF service can be used to select the *Origin* (2*).*

When the user is authenticated (3), the *Origin* assigns attributes which are presented to the *Target*. These attributes are proved as authentic since they are delivered through a secure communication channel (4). In case of successful authorization by the access control policy, access to the resources is granted (5). In some cases, additional attributes might be required in order to provide the services, and needed attributes are requested to the *Origin*. These attributes are sent only after getting the user's authorization. Within the architecture of Shibboleth, the privacy of the personal information is very important.

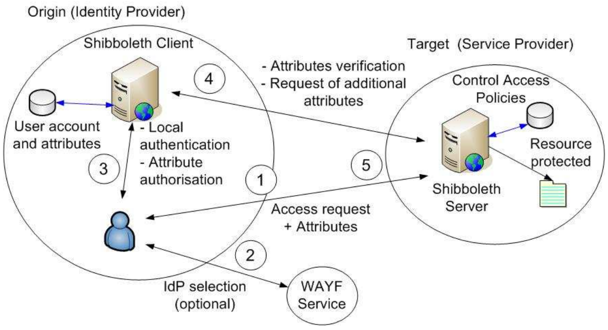
Origin (Identity Provider)
Shibboleth Client
User account and attributes
- Local authentication
- Attribute authorisation
3
4
- Attributes verification
- Request of additional attributes
Target (Service Provider)
Control Access Policies
Resource protected
Shibboleth Server
5
1
Access request + Attributes
2
IdP selection (optional)
WAYF Service

Figure 5. Elements of Shibboleth

As it can be seen, the identity information of the user resides solely in the *Origin*, but some attributes might be communicated to the *Target* who needs them for enforcing its access control policy. Therefore, an agreement concerning attributes and shared resources must exist between the *Origin* and the *Target*.

4. WS-Federation

Web-Federation is an important component within the secure framework architecture for Web Services. As we know, Web services is a mechanism that supports communication between web applications located in different organizations, and allowing the integration of applications in heterogeneous environment. Web Services bases its operation on the Service Oriented Architecture (SOA). Under this context, in 2002, IBM and Microsoft together with other companies defined a reference model to provide security to Web Services from a technological point of view as well as business activity policy [9].

4.1. Architecture

Figure 6 shows the security architecture model for Web Services:

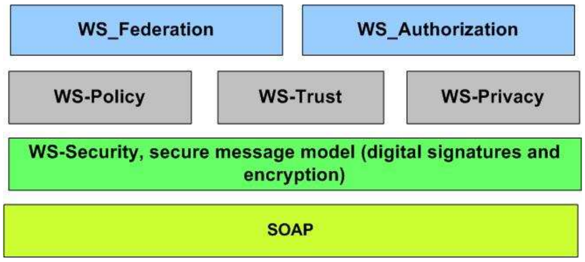
WS_Federation
WS_Authorization
WS-Policy
WS-Trust
WS-Privacy
WS-Security, secure message model (digital signatures and encryption)
SOAP

Figure 6. Secure architecture for Web Services

The security architecture for Web Services operates with the message transfer protocol of the Service Oriented Architecture Protocol (SOAP), the set of WS-Security definitions extends the functionality of SOAP to include security tokens within a SOAP message. In addition, it guarantees the integrity and confidentiality of the messages by means of the XML encryption and digital signature. The second level of specification (WS-Policy, WS-Trust and WS-Privacy) provides a framework to establish capacities and restriction policies, models of confidence and privacy preferences respectively. Finally, the WS-Authorization and WS-Federation specifications, define the elements necessary to build a Federated Identity Architecture [9].

4.2. Elements and operation

The WS-Federation model includes three elements: the Requestor (RQ), that is, an application requiring access to Web Services; the Identity Provider (IdP) or Security Token Server (STS) whose function is to carry out the authentication process and to transmit security tokens with relevant attributes; and the Resource Provider (RP) which is formed by one or more Web Services that provide the resource required by the Requestor [10]. Figure 7 shows the interaction between the different components of the architecture based on Web Services.

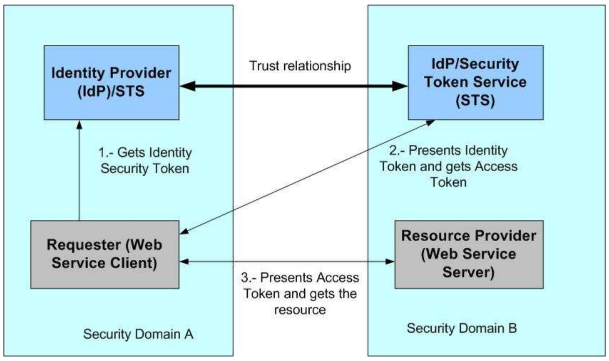
Identity Provider (IdP)/STS
Trust relationship
IdP/Security Token Service (STS)
1.- Gets Identity Security Token
2.- Presents Identity Token and gets Access Token
Requester (Web Service Client)
Resource Provider (Web Service Server)
3.- Presents Access Token and gets the resource
Security Domain A
Security Domain B

Figure 7. Relationship between the components of a Web Service architecture

When RQ in security domain A requests a web service located in another security domain (B in the figure), it is first authenticated by its Identity Provider and obtains a security token with its identity information (1). Depending on the requested web service, an additional access token may be obtained from the STS in security domain B with the necessary attributes to request the resource (2). Finally, the security token is presented to the Web Service (RP), who evaluates the security token and then applies its access control policy in order to grant access to the protected resource (3).

5. Initiatives comparison

The three Federated Identity Architectures presented in this paper have similarities and differences, as well as advantages and disadvantages depending on the context and usage cases. In the following paragraphs, a comparison is given in terms of their main functionalities.

Approach.- Liberty Alliance and WS-Federation are targeting business interactions whereas Shibboleth focuses on digital academic resource sharing.

Identity information storage.- Shibboleth is based on the centralized model where the identity information is centrally located and only attributes are sent to service providers. Liberty Alliance and WS-Federation, on the other hand, allow that the identity information could be distributed and federated in such a way that the authentication process could be done in any IdP within the Circle of Trust for a particular user.

Personal information privacy.- Shibboleth is the only architecture supporting the management of attributes trhough its *Attribute Release Policies* (ARP). In Liberty Alliance and WS-Federation architectures, attributes are divulged under the organization (IdP) control with little or no control from users.

SSO and web applications.- All the initiatives support SSO for web applications; however, Shibboleth only supports access to web applications from web browsers, whereas, WS-Federation is only designed for Web Services. Liberty Alliance supports both types of access.

Scalability.- WS-Federation might support a great number of users, IdPs and SPs. This is due to the flexibility of Web Services that may be easily programmed to behave as IdP or SP, and also their capacity to expand into big and complex structures. With Shibboleth and Liberty Alliance, the roles of the IdPs and SPs are well defined but the need for establishing a secure technological infrastructure and business agreement between the IdP and SP does not offer enough flexibility for building a big CoT.

User's security.- All the architectures are based on standards where the communication channels are encrypted and authenticated, thus guaranteeing a high level of security. However, the main problem is the identity theft which strongly depends on the security controls enforced at the user terminal. Some efforts within the initiatives are currently initiated.

6. FIA challenges

Despite some important advances carried out in the field, Federated Identity Architectures still face common challenges that represent very important issues for their real implementation. The following challenges can be mentioned.

Identity theft.- The theft of an identity represents one of the main issues because generally it remains undetected until the damage is done. In most of the cases, the identity theft does not occur over the communication channels, nor in the Identity Provider repository. It mostly occurs at the user terminal due to the lack of security mechanisms. Therefore research efforts must be allowed to improve robustness and security of terminals.

Privacy guaranty and legal compliance.- In some countries, laws do protect personal information against bad intended use. The current FIA initiatives have very weak definitions about how users might protect their personal information. An initiative called P3P (Privacy Preference Project) is proposed by W3C to define a standard for web sites to communicate their practices in terms of personal information collection, use, distribution and laws compliance [12]. These policies should be read by the web browser or in general by a user agent and be accepted / rejected on behalf of the user. This P3P standard could be advantageously integrated into the FIA initiatives.

PKI[1] integration.- PKIs are today largely implemented within companies to support every day enterprise transactions. One important challenge today for the FIAs is to provide integration with PKI so as to extend their functionalities in a transparent way.

AAA integration.- Operators are used to authenticate, and authorize users accessing their networks, and to perform communication accounting thanks to AAA protocols (e.g. RADIUS, Diameter). With their ability to identify users, and their large geographical coverage, they might serve as IdPs for any applications, and offer this extra identity management service to their subscribers. Moreover, operators are today used to operate inter domain AAA procedures, so that FIA might be naturally deployed over such AAA

[1] Public Key Infrastructure

architecture. Investigations on possible integration of AAA and FAI architectures are clearly needed.

P2P[2] application support.- Use of P2P applications has recently increased very fast. FIA introduction into P2P environment could bring security and a clean identification of P2P entities. However, integration is difficult today as FIA initiatives are based on a client/server model. The exchange of identity information in a P2P federated environment represents an important issue that must be fulfilled.

7. Conclusions

Digital identity management became a relevant security subject of importance due to the great amount and complexity of on line services that the user must interact with. Digital identity information must be exchanged between different organizations in a secure way for preserving personal information integrity and confidentiality. The Federated Identity Architecture tries to solve this problem. A FIA involves a set of technological solutions, as well as business agreements between organizations to conform to a trust structure that ensures the exchange of identity information. The most important initiative of FIA at the moment is Liberty Alliance, since its definitions include not only technological aspects, but also definitions related to business agreements in order to establish a Circle of Trust. This solution is focused on companies to strengthen B2B and B2C relations. Additionally, Liberty Alliance defines a complete framework to incorporate secure identity information exchange based on Web Services. The Shibboleth proposal is an academic approach where the main objective is digital resources between institutions without having to explicitly know the user identity, that is to say, it is an architecture where the privacy of the personal information is widely guaranteed and where most of the accessed resources are under an anonymous basis. Shibboleth is a framework simpler than Liberty Alliance, but it only solves a specific problem of collaboration and resource sharing between academic institutions. The WS-Federation initiative proposed by Microsoft and IBM focuses basically on the Web Services environment, taking advantage of the impulse made by the Service Oriented Architecture (SOA), which establishes an atmosphere of applications integration between organizations with heterogeneous infrastructures, WS-Federation adds security functionalities and allows the secure exchange of identity information of Web Services. None of these initiatives has consolidated as a unique solution and surely it will not be the case. Each initiative is focused on specific application area, thus they must interact so that jointly they provide a global solution. This subject opens a series of research lines that goes from improvements to the actual initiatives as mentioned in [11], to the proposal of new models that replace the present ones or new models that would allow their integration. Moreover research investigations are also promising targeting users' privacy and legal compliance, integration of FIA into current largely deployed PKI or AAA architectures, and FIA application to the P2P environment.

8. References

[1] A. Josang, S. Pope. "User Centric Identity Management". AusCERT Conference, 2005. pp 1-3.

[2] S. Subenthiran, K. Sandrasegaran, R. Shalak. "Requirements for Identity Management in Next Generation Networks". The 6th International Conference on Advanced Communication Technology, 2004. pp 138-142.

[3] S. Dongwan, A. Gail-Joon, S. Prasad. "Ensuring Information Assurance in Federated Identity Management". IEEE International Conference on Performance, Computing and Communications, 2004. pp 821-826.

[4] A. Bhargav-Apantzel, A. Squicciarini, E. Bertino. "Establishing and Protecting Digital Identity in Federation Systems". Proceedings of the 2005 workshop on Digital Identity Management, 2005. pp 11-19.

[5] T. Wason. "Introduction to the Liberty Alliance Identity Architecture", URL: http://www.projectliberty.org. Revision 1.0. Liberty Alliance Project, 2003.

[6] T. Jonathan, K. Yuzo. "Liberty ID-WSF Web Services Framework Overview". URL: http://www.projectliberty.org. Version 1.0. Liberty Alliance Project, 2004.

[7] T. Scavo, S. Cantor. "Shibboleth Architecture, Technical Overview". URL: http://shibboleth.internet2.edu/shibboleth-documents.html. Working Draft 02. June 2005

[8] S. Cantor. "Shibboleth Architecture, Protocols and Profiles". URL: http://shibboleth.internet2.edu/shibboleth-documents.html. September, 2005.

[9] Security Roadmap. "Security in a Web Services World: A Proposed Architecture and Roadmap". URL:http://www-128.ibm.com/developerworks/webservices/library/specification/ws-secmap/. IBM and Microsoft white paper. April 7, 2002.

[10] C. Kaler, A. Nadalin. "Web Services Federation Language (WS-Federation)". URL: http://www-128.ibm.com/developerworks/library/specification/ws-fed/. Version 1.0. July 8, 2003.

[11] W. Hommel, H. Reiser. "Federated Identity Management: Shortcomings of existing standards". 9th

[2] Peer To Peer

IFIP/IEEE International Symposium on Integrated Network Management. May 2005.

[12] S. Garfinkel, L. Faith. “P3P: Privacy Primer”. URL: http://www.oreillynet.com
/pub/a/network/excerpt/p3p/p3p.html. February 2, 2002.
.