Open IDM 2.0 Framework: a Unifying Gateway for Interoperable Identity Management

Brahim En-Nasry
Information Security Research Team
Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes, ENSIAS, Université Mohammed V-Souissi
Rabat, Morocco
ennasri@ensias.ma

Mohamed Dafir Ech-Cherif El Kettani
Information Security Research Team
Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes, ENSIAS, Université Mohammed V-Souissi
Rabat, Morocco
dafir@ensias.ma

***Abstract*—Today, as Internet has brought individuals and organisms within easy discovery and reach of each other, the role of identity has taken on great importance in social interactions, commercial transactions and governance. Interoperability as the foundation and key enabler for cross-domain Identity Management is still a complex challenge to achieve. However, efforts to build a unified framework for interoperability between Identity Management systems, that maps to different contexts such as business, government, real and virtual communities, will bring the breath solution that we all need. We investigate this issue from stakeholder's perspectives and across many technological initiatives approaches. Moreover, we also discuss advantages and drawbacks of some Identity Management systems with respect to interoperability standards. Finally, we highlight the interoperability requirements towards a unified model and motivate the need of a mature model for Identity Management and interoperability.**

Keywords - Security; Identity Management; interoperability; framework.

I. INTRODUCTION

Digital Identity Management tools are designed to ensure effective use of the multiple facets of identity and identification data associated to individuals in Internet transactions. Digital identity is multifaceted and also context sensitive. It contains strong identifiers that uniquely describe a person, as well as non-exhaustive lists of other attributes ranged from weak to strong and from temporal to persistent: relationships, reputation, preferences, etc. The early purpose of Identity Management Systems is to facilitate the establishment of security mechanisms. The ultimate goal is the control of access to assets, by supplying access control systems with reliable, up to date and consistent information, while granting a tradeoff between security, usability and privacy. In other terms, within an organization, an Identity Management System integrates many processes (authentication, authorization, accounting, identification and personalization) to interact with central repositories. In open environments, the implementation of a Digital Identity System differs depending on the approach adopted to meet trust requirements and expectations of various stakeholders.

The former Identity Management models, named "in silo", have been developed in closed environments, and are running with proprietary systems, without any possibility for interaction with each other. Within the rise in electronic data exchange in various contexts (such as business and consumer applications, Web 2.0, tele-declaration, etc.), it becomes necessary to bridge different Identity Management systems and manage different identities islets scattered in various accounts. Identity Management interoperability for networked and distributed applications continues to present several unique challenges for users and developers.

To take a look at the state of art, existing models are discussed in this paper, varying from centralized, federated to user-centric ones, reflecting their adaptation to Internet, through the evolution of service concept, and technologies to which they are associated. Each model requires some prerequisites and starts from a specific background [1].

Today, the storage and use of credentials (government issued credentials, credit card number, address, birth date, etc.) are controlled by the entity in possession of those credentials but in a confused manner. Without the distribution of defined roles and the delineation of the responsibility of each entity in all processes dealing with identity, interoperability can lead to the proliferation of solutions that spend the same problems.

A high level of interoperability can be reached if all entities in different domains can communicate to exchange identification information via a secure channel that permits strong and flexible authentication. This level must be reinforced by policies that define restricted roles and limits assigned to stakeholders. It is then useful to think about interoperability from a stakeholder perspective, including "user", "relying parties", and "ID providers" perspectives.

This paper is organized in 5 sections: after this introduction, Section 2 defines the global context of our study in terms of interoperability in current IDM approaches, especially under the scope of identity 2.0, in order to prepare the groundwork for an open interoperable IdM framework to access online services. Section 3 presents current approaches related to IDM existing frameworks. Section 4 proposes the model, consisting in a unified interoperable framework that will serve as a unifying gateway between all IdM solutions. Section 5 serves as a conclusion.

 ISBN: 978-1-61208-141-0

II. Interoperability in Current IDM approaches

In this section, we will discuss this problematic through the analysis of current Identity Management solutions and we will see if they can allow a certain level of interoperability.

But let us first give some precisions about interoperability from a stakeholder perspective, including "user perspective", "relying parties perspective", and "ID providers perspective":

- *User perspective:* In context of exchange between different systems, privacy of identity attributes is thus a crucial problem. The privacy paradigm is that individuals will be able to protect their privacy if their information can only be collected, used, and disclosed with their consent. Thus, users would like to choose their Identity Provider so that they can efficiently define attributes of their identity and securely control how these attributes are gathered, stored, shared among multiple service providers, with at least some level of portability;
- *Relying parties perspective:* RPs aim to cooperate each other, exchange accurate, up to date, and relevant information about individuals from any source to propose personalized services to better serve users from wide communities. At the same time, they want to delegate some identity administration tasks to IDPs. This new trend extends the security perimeter. Hence, they need to build trust relationships, protect their users and also their assets.
- *ID providers perspective:* IDPs want to provide identity as a service to users and relying parties and reinforce their positions as safe guardians of identity;

Current Identity Management solutions can be classified into 3 approaches:

A. Centralized approaches

Most of Identity Management systems deployed early in the Internet were client/server-based and called *silo models*. A single entity which operates the Identity Management system can be either the service provider acting as both service provider and identity provider or a trusted identity provider mixed up with service provider controlling together the name space for a specific service domain, and allocating identifiers to users. A user gets separate unique identifiers from each service/identifier provider he transacts with.

This approach might provide simple Identity Management for service providers, but is rapidly becoming cumbersome for users who will have to remember many identifiers and credentials associated to each service.

This approach has several drawbacks because the IdP not only becomes a single point of failure, but it may also not be trusted. The silo model is not interoperable and many of its aspects present serious deficiencies.

B. Federated approaches

A federated Identity Management system consists in software components and protocols that manage the whole life cycle of identities. In such a model, we assume that user data are stored at various locations on the Internet. This model supports many identity providers with no centralized control point. The distributed storage locations linked together are also easily shared. A federated model is a group of sites or systems that establish a trust agreement where each entity trusts identification data coming from others.

Federation facilitates the use of user attributes across trust boundaries as this architecture gives the user the illusion that a single identifier authority exists. Even if the user has many identifiers, he doesn't need to know them all.

With Single Sign On (SSO) mechanism, users authenticate themselves once by a federation member they trust, so they can navigate to any of the member service providers and be granted appropriate permissions based on their unique identifier shared among multiple service providers. The process of establishing a shared identifier for each user is often referred to as federating user's identities.

The level of interoperability within a federation is often fairly high, as they work better with seamless data transfer. The openness of a federation to new relying parties is more variable and depends on trust agreements, rules and the technology choices made by its designers.

Having different types of institutions as part of the federation (each with its own policies regarding its own users) makes it difficult for administrators to properly determine the categories of users allowed to access to each resource: Scalability is a potential problem unless the federation is relatively homogeneous.

Federations can cooperate with each other since they start to identify partners beyond their initial offerings. In this case, offerings to end users are improved substantially: but if the technology and rules used by federations are different, it can be difficult to implement cross-federation initiatives. A base level of interoperability is needed in order to broaden service availability provided by federations.

However, privacy protection is a serious problem, as it is difficult to know to which extent and under which circumstances federations driven by for-profit corporations will offer benefits to consumers. No one can grant if a company that holds customer data will not sell access to user databases to other online companies. A wide variety of federated systems are possible, so the consequences for both corporations and consumers of federation in general are uncertain. Relevant proposals, such as Liberty Alliance, Shibboleth, and WS-Federation, are based on the notion of federated identity. In Liberty Alliance, a federation consists in a circle of trust including service providers (SPs) and IdPs with mutual trust relationships. The circle of trust enables single sign-on (SSO) across different SPs' websites. When an SP requests user authentication, the IdP authenticates the user and then issues an authentication assertion. The SP validates the assertion and determines whether to accept it. The unique first authentication of a user is enough to sign on to other service sites.

 ISBN: 978-1-61208-141-0

C. User-centric approaches

User-centric models [2] are driven by privacy concerns and aim to leave control with the user as to initiate or approve any transfer of personal information before it takes place, either directly or through a mediator with predefined rules for authorization. A user-centric model must have a basic level of interoperability in order for an individual to use their digital ID for multiple services.

Though data can still be stored with a relying party once data is given in a transaction, this model allows individuals to disclose minimal information. The information provided by the user can be easily checked with the Identity Provider, causing greater accuracy and less potential for fraud.

A major drawback of the user-centric model is its complexity. There are significant technical challenges related to creating a system that sufficiently satisfies all parties, so that they actually use it. One should not forget also social challenges in educating business owners and users. Most web businesses are accustomed to asking users to provide identifying information – often more than strictly necessary – and users are used to providing it, and setting up a username and password for each site. This situation is familiar, if cumbersome.

In contrast, a user-centric model requires both user and relying party to develop relationships with one or more trusted Identity Providers and possibly install and learn new software. This attitude could be a barrier to widespread adoption. Furthermore, businesses that currently collect identifying data may be reluctant to give up control over their customers' data, by using it for marketing or selling it to direct marketers.

Interoperability between user-centric and non user-centric systems is not always possible due to the preconditioned circle of trust and trust agreement requirements.

III. Current existing frameworks to interoperability

Many initiatives are currently under work to develop the Internet-based Identity Management services called Identity 2.0. They are based on the concept of user-centric Identity Management, supporting data mapping, authentication and identity verification protocols while protecting privacy by letting user with a margin freedom to express her consent and control her identities when doing Internet-based transactions. Until now, there are two categories of Identity 2.0 initiatives: URL-based and Infocard-based. The main difference among such proposals is the protocol they use to verify user identity. In CardSpace, the user selects from a set of information cards representing the digital identities that satisfy a relying party's (RP's) policy. The identity provider (IdP) that issued the card releases to the user a security token, encoding claims corresponding to the selected information card. The user then passes the card and the token to the RP. Credentica and CardSpace support similar identity verification protocols: The RP verifies the user's identity based on an IdP issued ID token, encoding claims about the identity presented by the user to the RP.

Contrariwise, OpenID is a URL-based protocol and when users access an RP's website, they provide an OpenID that is the URL of a webpage listing their IdPs. The RP selects an IdP, and the browser is redirected to the IdP's webpage.

If the IdP successfully verifies the user's identity, the browser is redirected to the designated return page on the RP website, along with an assertion of user authentication.

We should not forget that the frameworks listed below are unified solution to interoperability. They just propose initiatives to solve some aspects of interoperability within Identity Management approaches. Higgins is a model that will be useful, if modified to become a powerful bridge between many models.

A. XRI

The Organization for the Advancement of Structured Information Standards (OASIS) has developed a unified identifier scheme to help companies tackle today's rampant Identity Management interoperability problems.

The Extensible Resource Identifier [3] (XRI) specification establishes an interoperable framework for expressing, resolving and establishing equivalence between identifiers of any kind for any resource type, including people, applications, network devices and corporate assets. XRIs build on the ubiquitous Uniform Resource Identifier (URI) and Internationalized Resource Identifier (IRI) standards - widely used by Identity Management solutions - by defining standard ways to express characteristics such as type, language and date. The lightweight HTTP- and XML-based XRI resolution framework lets a consuming application quickly and easily discover metadata related to resources, such as an alternative synonym identifier that works better in the application's local Identity Management system.

Metadata isn't limited to alternative identifiers. Imagine that an XRI-identified resource is a technical manual, available as a PDF or Word document and retrievable from a variety of mirrored network locations via various protocols.

In a broad sense, the manual is the same document irrespective of where it is located, how it is retrieved or in which format it is represented. XRIs are ideally suited for identifying resources at this level of abstraction because the resolution process lets the consuming application choose the best network location, retrieval method and file format for its needs from the available options.

Like URIs, XRIs are composed of an authority portion and a path portion. XRI resolution converts the authority portion and the path portion of an XRI to an XML document called an XRI Descriptor. The XRI Descriptor describes the identified resource and the means by which the digital representation of the resource can be retrieved.

By providing an additional level of in direction away from concrete instances of a resource, XRIs provide a permanent, unbreakable reference on which stable business relationships can be based.

 ISBN: 978-1-61208-141-0

B. SAML

The initial versions of SAML [4] v1.0 and v1.1 define protocols for SSO, delegated administration, and policy management. The most recent version is SAML 2.0. It is now the most common language to the majority of platforms that need to change the unified secure assertion. It is very useful and simple because it is based on XML.

This protocol enables interoperability between security systems (browser SSO, Web services security, and so on). Other aspects of federated Identity Management as permission-based attribute sharing are also supported.

C. Identity Web Services Framework

In the second phase, the specifications offer enhancing identity federation and interoperable identity-based Web services. This body is referred to as the *Identity Web Services Framework* (ID-WSF). This framework involves support of the new open standard such as WS-Security developed in OASIS. ID-WSF is a platform for the discovery and invocation of identity services - Web services associated with a given identity. In the typical ID-WSF use case, after a user authenticates to an IdP, this fact is asserted to an SP through SAML-based SSO. Embedded within the assertion is information that the SP can optionally use to discover and invoke potentially numerous and distributed identity services for that user. Some scenarios present an unacceptable privacy risk because they suggest the possibility of a user's identity being exchanged without user's consent or even knowledge. ID-WSF has a number of policy mechanisms to guard against this risk. But ultimately, it is worth noting that many identity transactions (automated bill payments) already occur without user's active real-time consent (users appreciate this efficiency and convenience).

As a standard, SAML supports a standard syntax for the representation of assertions about identity attributes and IdP authentications but does not provide an identity verification protocol. SAML is important in our approach as it facilitates the exchange of identity tuples and mapping certificates across domains in a federation.

To build additional interoperable identity services such as registration services, contacts, calendar, geolocation services, and alert services, it's envisaged to use ID-WSF. This specification is referred to as the *Identity Services Interface Specification* (ID-SIS).

D. Shibboleth

Shibboleth [5] allowed interoperation between academic institutions by developing architectures, policy structure, practical technologies, and open-source implementation.

E. OpenID 2.0

OpenID authentication 2.0 [6] is becoming an open platform that supports both URL and XRI user identifiers. In addition, it would like to be modular, lightweight, and user oriented. Indeed, OpenID auth. 2.0 allows users to choose, control and manage their identity addresses. Moreover, the user chooses his identity provider and has a large interoperability of his identity and can dynamically use new services that stand out, such as attribute verification and reputation, without any loss of features. No software is required on the user's side because the user interacts directly with the identity provider's site. OpenID Authentication provides a way to prove that an end user controls an Identifier. It does this without the Relying Party needing access to end user credentials such as a password or to other sensitive information such as an email address. OpenID is decentralized. No central authority must approve or register Relying Parties or OpenID Providers. An end user can freely choose which OpenID Provider to use, and can preserve their Identifier if they switch OpenID Providers. OpenID Authentication is designed to provide a base service to enable portable, user-centric digital identity in a free and decentralized manner. It uses only standard HTTP(S) requests and responses.

The exchange of profile information, or the exchange of other information, can be addressed through additional service types built on top of protocol to create a framework.

F. InfoCards

CardSpace is Microsoft's code name for this new technology that tackles the problem of managing and disclosing identity information [7]. CardSpace implements core of identity meta-system, using open standard protocols to negotiate, request, and broker identity information between trusted IdPs and SPs. It is a technology that helps developers integrate consistent identity infrastructure into applications, Web sites, and Web services.

G. Higgins

Eclipse Foundation [8] has developed an open framework built around info-cards, to enable user's interaction with multiple authentication protocols. This framework allows software developers to use identity cards as a form of authentication to integrate and leverage multiple identification protocols within their applications. Three components provided by Higgins for enabling information-card authentication:

1) Identity selector applications: end-users can use to sign-in to web sites and systems that are compatible with Info-Card-based authentication.

2) Complete code: necessary for Identity Provider web services as well as for the "relying party", it enables websites and systems to be information card- and Open Id-compatible. Software developers can incorporate this code into their applications to make it easier for their users to login to their site. There are currently two web-site developer solutions available (STS, IdP-for, WS-Trust and SAML2 IdP –for SAML2)

Higgins Global Graph (HGG) data model and the Higgins Identity Attribute Service (IdAS): Developers now have a framework that provides an interoperability and portability abstraction layer over existing "silos" of identity data. The HGG/IdAS layer of Higgins offers integration opportunities between several identification protocols such as OpenID, WS-Trust, SAML, and LDAP.

 ISBN: 978-1-61208-141-0

IV. "OPEN IDM": A UNIFIED INTEROPERABLE FRAMEWORK

A. Motivation

To reach a basic level on interoperability, federated identity solution must, by its very nature, be standards-based. The key underlying standard for federated identity is SAML. SAML is the most mature and widely deployed identity federation protocol today and offers the highest potential for interoperability with federation partners. The latest version, SAML 2.0, marks the convergence of the SAML, Liberty ID-FF, and Shibboleth specifications into a single unified standard. A federated model must be user centric to allow the user to maintain control over its identity.

Distributed solutions are also interoperable and user centric if they use the same approach and technology. Level two is possible if at least two approaches are interoperable.

B. Proposed Unified framework

Interoperability between multiple Digital Identity systems has become an important and complex issue. Even if many initiatives exist, high level interoperability is far from being achieved outside circles of trust. Existing models are not clearly interoperable and are deficient in unifying standard-based protocols due to the conflicting requirements for each approach. In untrusted domains, privacy concerns and user's attribute controls are fundamental when offering identity to users; on the other hand, the same users ask for flexible access through homogenous user friendly interfaces. Taken as a single solution, it may not exhaust all possible solutions to the issue, but when bridging all solutions, this approach will federate all efforts currently under development.

From a logical point of view, high level of interoperability will be assured by a unified framework, an open user-centric bridge managed by a new entity so called Master Identity Provider (Figure 1). This framework serves as a unifying gateway between all existing models. In one side, as industry and other organizations continue to introduce capabilities and standards guided essentially by the approach adopted and suitable for only one specific community within a specific context, but not for all possible use cases. In other side, all identity problems come from the lack of visibility towards IDPs that work separately without any well-defined relationships between them.

Thus, a Master Identity Provider acting as a Root Authority to identities, will federate all relationships between IDPs in order to build the identity, during enrolment processes, piece by piece starting with the root while avoiding any duplication and any unnecessary information which represents nothing.

This unified framework serves as a metasystem to bridge all scenarios of Digital IDM Systems, which must be interoperable. This new arrangement of accepted standards enables decentralized identity infrastructure to work together as a single Identity Management system, including:

1) *External standards:* such as XML, SAML, etc.
2) *Open Software standards:* such as java or Linux
3) Hardware standards: they support interoperability

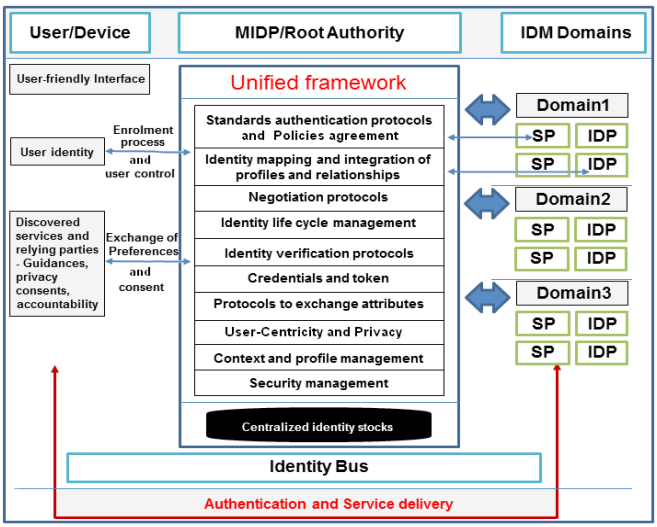

Figure 1. Architecture of the proposed framework

C. "Open IDM 2.0" Framework modules

1) Policies agreement module: it includes Service Provisioning Policies, Service Provider Privacy Policies, Privacy Preferences and Federation Agreement Policies.

2) Identity mapping and integration of profiles and relationships module: A first step toward achieving interoperability is the adoption of a standard to describe assertions and identity profiles.

3) Negotiation protocols module: it integrates all negotiation aspects especially trust negotiation when entities are not previously known to each other. Before meaningful interaction starts, a base level of trust must be established.

4) Life cycle management module: All federated identity solutions must provide management capabilities to perform required tasks to create, provision, manage and monitor it.

5) Security module: manages all security concerns.

6) Heterogeneous identity verification: heterogeneity among identity verification protocols and naming, especially in the context of the clients' identity verification process. It specifies such a set of identity attributes. If clients use names for the identity attributes from different vocabularies, after a client request for a resource or a service from an RP, they may not understand the adequate identity attributes.

7) Security Credentials and Token module: it supports different identity tokens and related encryption algorithms.

8) Protocols to exchange attributes: this module enables exchange of attributes in a cryptographic way

9) User-Centric and Privacy module: Users should have the maximum control possible over the release of their identity attributes. They should state under which conditions these attributes can be disclosed.

10) Context and profile manager: identity and context are closely related; during interoperability analysis, context issue must provide consistent experience across contexts.

11) Centralized identity stocks: playing the role of a repository in order to concentrate all IdM resources.

 ISBN: 978-1-61208-141-0

The proposed unified framework interacts with the global IDM architecture, through the following elements:

- *User Identity:* relates to a person, device or application, in order to define identity strength.
- *Identity Bus:* supports interoperability between varieties of IDM technologies available from different vendors, an Identity Bus that will provide interoperability functionalities is necessary.
- *Consistent user interface:* Lack of usability will make the control of identity by user almost impossible to take place. The model must facilitate the developer with adequate support for implementing usability through a user interface.

D. Analyzing the Framework

Trustworthiness of an identity depends on the initial enrollment process, the security token being issued, the level of collaboration and the depth of the relationship between entities. As identity providers and relying parties in current ecosystems don't directly communicate during enrollment process, identity islands remain as data silos between each other. This framework as a harmonized identity metasystem aims to solve the problem of consolidation of distributed identity and provide secure, privacy enhanced and seamless experiences. Reasonable-diligence of services needs to validate the identity of individuals or organizations requesting credentials that will enable them to participate in information exchanges. Trust will convey through inter-domain exchange of identity attributes as well as any useful information and policies to collaborate in tracking down all identity transactions.

To consolidate identity, we acknowledge that an Open IDM framework should integrate -but should not be limited to- the two main following processes :

Enrolment process required by a service*:* in Figure 2, (1) user contacts SP (2) user is redirected to the IDP which SP trusts. (3) SP specifies to his IDP what attributes it needs. (4) IDP contacts his direct MIDP where user is referenced and user is redirected to MIDP to be identified. (5) If the user is really referenced, a profile negotiated with user is generated with respect to the principle of minimal disclosure. (6) MIDP provides IDP with minimal attributes and new credentials are issued.

Access to service: a user attempts to gain authorization to do something online. User contacts MIDP to know if service is referenced and user already enrolled. Authentication is activated towards IDP with adequate protocol and credential.

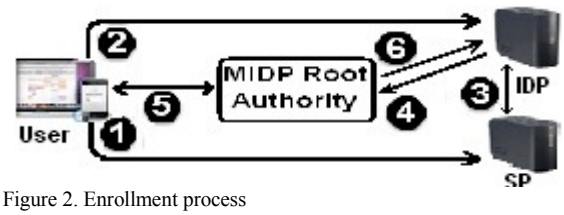

Figure 2. Enrollment process

This proposed framework presents many advantages: True interoperability will be possible with the open gateway serving as interface to standard protocols.

- Technologies like OpenID, SAML, Liberty ID-FF and WS-Trust should be supported. Data format and authentication systems at endpoints support new credential arrangements. Data is decoupling from application and IDM layer from application layer.
- User control empowerment: users have full knowledge regarding information they disclose.
- User preferences customize relying parties services

Our framework presents drawbacks, such as the unifying gateway. This point of failure will be a part of future work.

E. Implementation issues of the framework

This framework encompasses several modules. Research will now develop all those components and proceed towards the implementation and evaluation of associated prototype solution. Modules and interactions between platform components will be developed, implemented and tested successfully. Investigations will be conducted to select components supporting proposed aspects.

V. Conclusion

This article discusses ongoing concerns with the interoperability between different Identity Management solutions. Current solutions are developed independently but their functionality complement each other. This unified gateway will exploit all specifications to define new standards to encapsulate different protocols.

In future work, as part of the PhD thesis, we'll tackle description for options and parameters of protocols and how parameters are interpreted and mapped to each other.

Bringing a Unifying Gateway for Interoperable Identity Management as a response to interoperability challenges will enhance trust and encourage the wide use of identity systems. But, Trust relationships have to be established.

Acknowledgment

Authors thank University Mohammed V-Souissi, for supporting this work (research project 006/ENSIAS/2011).

References

[1] E. Bertino et al. "Identity Management: Concepts, Technologies, and Systems", pp. 110-111, Artech House, 2011

[2] R. Marx et al. "Increasing Security and Privacy in User-centric Identity Management: The IdM Card Approach", *2010 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing,* pp. 459-464, IEEE, 2010

[3] P. Mishra et al. "*Conformance Requirements for the OASIS Security Assertion Markup Language V2.0"* OASIS SSTC, 19 pages, March 2005

[4] OASIS (Organization for the Advancement of Structured Information Standards) project: http://www.oasis-open.org, 2011

[5] G. Connor, "Shibboleth: A Templar Monitor", Kessinger Publishing, 216 pages, 2010

[6] D. Recordon et al., "OpenID: The Definitive Guide: Identity for the Social Web", 225 pages, O'Reilly Editions 2011.

[7] V. Bertocci et al. "Understanding Windows CardSpace: An Introduction to the Concepts and Challenges of Digital Identities", 384 pages, Addison-Wesley Progessional, 2008

[8] *Higgins Personal Data Service:* http://www.eclipse.org/higgins*, 2009*

 ISBN: 978-1-61208-141-0