Security for Future Networks : a Prospective Study of AAIs

Hassane Aissaoui, Pascal Urien, Guy Pujolle, Fraga Joni da Silva, Böger Davi da Silva

Security for Future Networks : a Prospective Study of AAIs

Hassane AISSAOUI MEHREZ, Pascal URIEN
TELECOM-ParisTech : LTCI CNRS Laboratory
IMT / TELECOM-ParisTech
46, rue Barrault F 75634 Paris France

Guy PUJOLLE
CNRS, LIP6/UPMC Laboratory,
University Pierre and Marie Curie Paris VI
4 Place Jussieu, 75005 Paris, France

Joni da Silva Fraga, Davi da Silva Böger
Universidade Federal de Santa Catarina,
Centro Tecnológico, Departamento de Engenharia Elétrica.
LCMI/DAS/CTC - UFSC, C.P. : 476 88040-900 - Florianopolis, SC Brasil
E-mails: {hassane.aissaoui, pascal.urien}@telecom-paristech.fr, guy.pujolle@lip6.fr, fraga@lcmi.ufsc.br.

Abstract:

The future Internet will rely heavily on virtualization and cloud networking. The project Security for Future Networks proposes the design of a framework providing secure identification and authentication, secure data transfer and secure virtualized infrastructure.

In this paper, we present a comparative study should examine some models and frameworks of Identity Management (IdM). Initially, we had identified OpenID, Higgins and Shibboleth frameworks as those providing facilities that are the closest to our proposals. However, with the literature prospection more frameworks have being included in our study, which has allowed to expand our state of the art on IdM. In the study, presented in this paper, some OpenId features are highlighted and related with our objectives.

Keywords: Security, Virtualization, Cloud Networking, Microcontrollers, AAIs, User-Centric Controls, Identity management, Single Sign-on.

1. Introduction:

The project Security for Future Networks (SecFuNet) [1] proposes solutions for integrating secure microcontrollers in a global and secure Identity Management (IdM). The IdM system will be based on several local authentication servers composed by secure microcontrollers. Initially, some requirements were defined to this project; such as User-Centric and Federated Identities approaches for the IdM.

Among the security and reliability requirements, privacy and intrusion tolerance are special issues that will be treated with considerable efforts. IdMs based on federated identities deliver defined policies for releasing user attributes that often threaten user privacy. It occurs mainly because the idea of federations is centered on information sharing.

The objective of this paper is a prospective study of frameworks and models of IdM. Our comparative study examines some models and frameworks of IdM illuminated by the main concerns and requeriments of the SecFuNet Project.

The rest of this paper is structured as follows. The main concepts and approaches to IdM models are described in Section 2. Section 3 describes what level of assurance (LoA) means and which factors affect this parameter. Next, Section 4 compares different solutions of IdM models and overviews infrastructures supporting these models. The discussion presented in this paper is driven for metrics and attributes derived from some of requirements cited above. In Section 5 final considerations about the benefits provided both to users and service providers, when identity and User-Centric models are used in identity management, Section 6 conclusion and the overall description of the first choice of the solutions that will be used in this project.

2. Related work

The identity of a user (or a person) may consist of a large amount of personal information that characterizes this person in different contexts in which he takes part [2]. The identity may be considered as a combination of sub-sets of so called partial identities, some of which uniquely identify a person (eg, social security number) and others not. Depending on the context and situation, a person may be represented by different partial identities. The partial identity of a user in the context of a university can contain information such as name, birth date and lectures that he attends. Within a company, the identity can be associated with roles, privileges, rights and responsibilities. It should be noted that the same personal information may be present in different partial identities of the user.

An IdM system provides tools to manage partial identities in a digital world. IdM is used to ensure the entity associated to a digital identity and also, for delivering authenticated information contained in the corresponding identity [3].

While in the real world a person chooses what information about himself to reveal to others, taking into account the context and sensitivity of the information, in the digital world, this task is performed by the IdM system.

2.1. IdM Features

An IdM system integrates identities, attributes and policies, resulting in mechanisms for authenticating users and delivering attributes for business processes. Usually, an IdM is decomposed in the following elements [4]:

- *User* - the one who wishes to access a service;
- *Identity* - a set of attributes that characterizes a user into a digital world. It can be his name, address, affiliation, etc.;
- *Identity Provider* (IdP) - responsible to maintain user registers and for issuing identifiers associated to users. After an authentication process with the Identity provider, the user receives a credential, or an authentication assertion, which is recognizing him as valid or known user in the domain of the identity provider;
- *Service Provider* (SP) - provides resources to authenticated (or recognized) users. In other words, the user may access SP resources after having verified the authenticity his. For having the resource access liberated, SPs may also demand some special user attributes what characterizes attribute-based access controls.

2.2. Identity Management Models

IdM systems models are classified as traditional, centralized, federated and user-centered [4] [5]. Figure 1 illustrates each model and their interactions in authentication procedures.

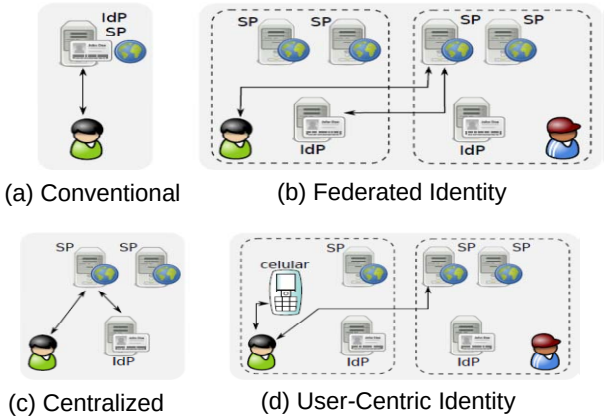

Figure 1: Identity Management Models

In *the conventional model*, the identities (IDs) are individually handled by each service provider, which also plays the role of an identity provider (see Figure 1.a). A user creates his or her digital identity (ID) for each service provider (SP) with which he/she interacts. Usually, user IDs are not shared among different service providers and this approach tends to be costly for both users and service providers. Each service provider may require its own set of attributes to form the digital identity of the user. On the other hand, a common set of attributes may be required by many service providers, such as account name, password, address, date of birth, etc.

For users, managing multiple of identities is somewhat costly. First by having to provide the same information several times and second by having to worry to create a username and different password for each service provider, since to use the same password for different providers is not advised. The cost generated to users may also be reflected in future problems. The tedious task to always provide the same information at the time of creation of their account in the SP causes the user not to be so more careless or inaccurate in filling asked attributes that can be crucial to access the resource offered by the service provider.

The *centralized model* appeared as an alternative solution to the inflexibility of the conventional model. It is based on the sharing of user identities between service providers and on the concept of single authentication or Single Sign-on (SSO). The Microsoft Passport Network was a precursor of this model which tried to avoid inconsistencies and redundancies in the conventional model, giving users the ability to interact with various services providers without the need to perform the authentication process in each of these services.

In the centralized model, all service providers that have trust relationships with an IdP (an identity provider or an authentication authority), must rely completely on the user authentications provided by this IdP (see Figure 1.c). The identity provider is responsible for authenticating users and supplying user's attribute to service providers. The concept of single authentication (SSO) represents a great convenience to users since they only need perform the authentication process once and thereafter they can use the obtained credentials on all service providers they wish to access, until these credentials expire. The weak point of the centralized model is that the provider identity has absolute control over the information of its users, and may use their information in any way he wants [6].

This is the main reason why Microsoft Passport Network has not been successful.

In order to avoid the deficiencies presented by the centralized model, the *federated identity* model was introduced based on the distribution of the task of user authentication across multiple identity providers. These identity providers are arranged in different administrative domains (see Figure 1.b). An administrative domain can represent a company, a university, etc. and is composed of users, many service providers and a single identity provider (IdP). The concept of federated identity relies on trust relationships which are established among multiple identity providers (IdPs).

The federated identity model is an approach which optimizes information exchanges in user authentications through IdPs' trust relationships [7]. These agreements between IdPs ensure that identities issued in a domain will be recognized by SPs in other domains. Thus, the identity federation model can offer facilities to users because it relieves them of having to deal with diverse identities and to execute many times the authentication process. The benefit of federated model is that it can handle a smaller number of users' information.

The user-centric model aims give to the user total control over its digital identities, but the main proposals and implementations of this model are built using any of the previous models presented above. However, the user-centric approach is most widely used with the model federated identity. Each identity of a user is stored on a physical device which is held by the user, such as a smartcard or even a cell phone (see Figure 1.d). The user authenticates him in this physical device and may choose what identity he wants to use with a specific service provider. This approach fully respects privacy preferences of the user.

2.3. Requirements for an Identity System

A set of requirements [8] for identity management systems is listed. These requirements should be met for ensuring more flexibility and performance to users without affecting the security of their personal information. The requirements listed are: *interoperability, mechanism for revoking identity, management of trust relationships, privacy and anonymity.*

2.4. Levels of assurance to user authentication

The U.S. National Institute of Standards and Technology (NIST) has released a guide on authentication process [9] which defines *four levels of assurance (LoA). Level 1 is considered the weakest and level 4 the most robust*. The corresponding documentation indicates the technical requirements for each level summarized, below, in tabular form. Table 1 shows the different kinds of tokens that may be used at each authentication assurance level. Table 2 identifies the types of authentication protocols that are applicable to each assurance level.

For example, an authentication process that makes use of user name and password is considered less robust than a process that makes use of hardware device that contains a protected cryptographic key. Service providers could use these levels to provide different levels of authentication and authorization.

Token type	Level 1	Level 2	Level 3	Level 4
Hard crypto token	√	√	√	√
One-time password device	√	√	√	
Soft crypto token	√	√	√	
Passwords & PINs	√	√		

Table 1: LoA allocated to each Token Types

Protocol Type	Level 1	Level 2	Level 3	Level 4
Private key PoP	√	√	√	√
Symmetric key PoP	√	√	√	√
Tunneled or Zero knowledge password	√	√		
Challenge-response password	√			

Table 2: Authentication Protocol Types

3. An Overview of the main AAI

3.1. SAML:

SAML (Security Assertion Markup Language) [10] is a computer standard defining a protocol for securely exchanging identity information (*authentication, authorization and attributes*) among applications regardless of the technologies used by each application (PKI, SSO, LDAP, Kerberos, etc.). Version 2.0 of the specification was standardized in May 2005, by OASIS (Organization for the Advancement of Structured Information Standards) Security Services Technical Committee (SSTC).

The current version (2.0) extends the former infrastructure with concepts and mechanisms derived from other projects (ID-FF V1.2: Liberty Alliance Identity Federation Framework) and Shibboleth V1.2 of Internet2 Consortium that have broader goals, such as the creation of federations for sharing security information and the IdM.

3.1.1. Secure exchange of the identity information

The core of SAML is an XML grammar for representing security information in assertion formats [11]. SAML specifications define five components (Figure 2):

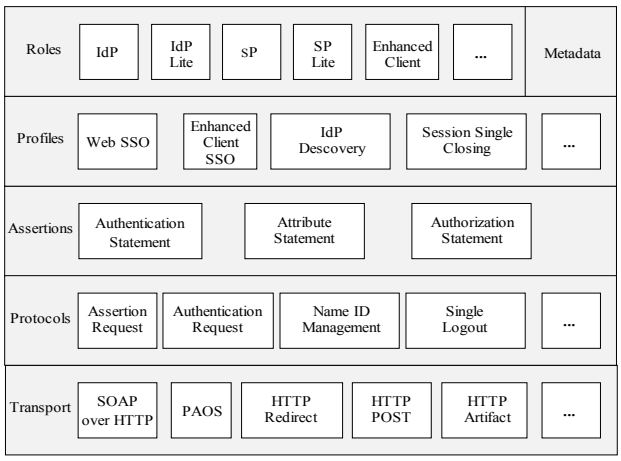

Figure 2: SAML Architecture [12]

The *roles* define the roles that each entity can play in SAML infrastructure, and in additional the metadata describe these entities in this architecture.

Profiles describe the protocols and assertions to specific data transfers for providing IdM and single authentications.

Assertions specify the format to represent security information about a subject which may be a person, organization, computer, etc and are essential to IdM and security contexts.

Protocols and Transport defines in two layers messages and transport protocols: XML schemas for SAML messages are described in the top layer (*Protocols*). The bottom layer (*Transport*) consists of specifications defining how to use the underlying protocols (SOAP, HTTP, etc.) to transport these SAML messages [13]. They SAML messages are used to request and transfer assertions between entities. These protocols can be mapped to different *"transport"* mechanisms.

SAML provides functionalities and mechanisms for implementing any approach of identity management. SAML Federations may be established using SAML metadata for describing trust relations among IdPs.

3.1.2. Privacy in SAML Federations

In early SAML versions few mechanisms were available to *preserve privacy* in IdM approaches that emphasize sharing user information. However, SAML 2.0 provides support to the use of *pseudonyms*, which are *dynamic identifiers* and not related to the identity attributes of the subject. Pseudonyms serve as identifiers shared between SP and IdP and can be used in two ways: *persistent and transient*.

The *persistent pseudonym* is created once at the IdP and associated permanently to a subject identity. This scheme, combined with the privacy policies on access to subject attributes, can guarantee identity protection. However, access to different SPs can still be tracked if these SPs act in collusion.

The *transient pseudonym* is created by the IdP and associated with the identity of a subject for the duration of a computing session of the user. Thus, the SP can still decide the subject access based on attributes issued by the IdP, but can no longer afford information about the subject that persist for more than one session. Moreover, SP cannot correlate different sessions of the same subject, ensuring a certain level anonymity.

3.2. WS-Trust

WS-Trust specification [14] introduces a protocol for exchanging security credentials among different security domains. *WS-Trust* also provides means for checking whether a credential can be trusted or not, so that user and SPs evolved in interactions can detect and extend trust relationships based on the credential emission and validity checks. The trust model defined in *WS-Trust specification* is based on the Security Token Service (STS). The STS is a Web Service that implements a standard WSDL interface, where operations for the emission, renewal, validation and revocation of credentials are defined. Thus, the STS serve as a trust mediator between the different security domains.

In general, the trust model of *WS-Trust* specifies that a service provider may require that a message includes proof

of a set of claims, in the form of security tokens, before being processed. The requirements imposed by the service provider translate into a set of supported security tokens and a set of trusted STSs. If the message contains enough security tokens, emitted by trusted STSs, that cover the required claims, the service provider continues the processing. In order to make the service dynamic and interoperable, security requirements should be described in policy documents expressed in a standard format, such as WS-Policy [15]. These policies should be also attached to the WSDL description of the service. The messages exchanged by STS are quite general and allow extensions and future compositions.

3.3. WS-Federation

WS-Federation specification [16] is an OASIS standard that defines mechanisms based on the WS-* standards, especially WS-Security, WS-Trust and WS-Policy, for the construction of federations. These standards already define the basis for managing federated identities, but the WS-Federation proposes extensions that define how to combine these models in order to provide richer functionality to the security domains (or administrative domains) in and across federations. WS-Federation allows federated IdM and like SAML, provides a similar set of features. WS-Federation provides SSO, Single Logout (SLO), attribute exchange (based on privacy policies), permanent and transient pseudonyms and metadata documents.

3.4. Shibboleth

The Shibboleth project was an initiative of the Internet2 U.S. consortium [17]. It was developed to be a generic solution to federated identity management, which may be adopted by any type of organization.

Shibboleth is a software package based on open standards such as XML and SAML and provides an easy way to enable applications to use facilities of a federated identity model such as, for example, the concept of SSO and secure exchange of user attributes for service providers that take part of a Shibboleth federation. Several functionalities not specified on SAML 1.x were implemented in Shibboleth in order to provide SSO. Most of these features were incorporated by SAML 2.0 and current versions of Shibboleth (starting from 1.3) are fully compliant implementations of several SAML profiles.

Shibboleth has an emphasis on the privacy of users' attributes. The release of these attributes for service providers is restricted by the privacy policy of the origin domain and also by user preferences.

There are three main roles within a Shibboleth domain: Identity Provider (IdP), Service Provider (SP) and Discovery Service (DS). The first one is responsible for authenticating their users before they can make use of the services offered by the second. In Shibboleth, the authentication process is always performed at origin domain of the user, through his identity provider, making use of authentication mechanisms present in his organization (or domain). The authentication of users can be done through username and password, Kerberos, X.509, etc. Although most of the time both IdP and SP implement the entire software stack provided by the Shibboleth project, it is possible to use other solutions that are compliant with SAML 2.0. This allows user credentials to be transported from the identity provider to provider services. The Discovery Service also called “Where Are You From?” (WAYF) is an additional component that allows the user to choose an IdP in multi-domain architecture of identity. The WAYF can be used by the SP to determine the user's preferred IdP with or without user interaction. Shibboleth is usually used for implementing academic federations.

3.5. Liberty Alliance

The Liberty Alliance Project has emerged in order to create open specifications for the management of federated identities. These specifications were addressed to the integration with Web Services applications [18]. One of the main strengths of this project is its influence on standards such as SAML, whose extensions proposed by Liberty Alliance are now part of SAML 2.0 [19].

3.6. OpenID

OpenID is an identity management framework that is lightweight, scalable and extensible. It is maintained by OpenID Foundation, a nonprofit organization that promotes technological development. It is based on Web standards like HTTP and URIs and provides for user-centric identity management and SSO authentication. The basic idea of OpenID is that a user may access a Web site if he is able to demonstrate that he controls an OpenID identifier. This identifier (or handle) is usually a URL (Uniform Resource Locator) or, in some cases, an XRI (Extensible Resource Identifier).

OpenID operation is based around an authentication protocol where OpenID Providers issue assertions that prove a user owns a given identifier (an OpenID). Such assertions are consumed by service providers in order to give the user access to services. OpenID authentication protocol specifies the message exchanges used in order to fulfill the authentication process.

3.7. OAuth

OAuth comes from the social web, with version 1.0 (RFC 5849) which dates from 2007. It allows a user to access resources located on another site without disclosing its identifiers / passwords. A third party site acts on behalf of the user. OAuth version 2.0 is not backward compatible with OAuth 1.0. OAuth 2.0 is open to the domain of business and Cloud, enabling and incorporating specific use cases that make it suitable for authentication and authorization with REST API (REpresentational State Transfer) [20]. OAuth is becoming widespread in the web authentication domain. One of the strengths of the system is the simplicity with which the information is centralized and authenticated. OAuth protocols are used in many different service providers, such as Gmail, Twitter, Facebook and others.

3.8. Higgins Project

The initial motivation for the Higgins project was to implement a identity management system based on the user-centric model. In other words, this framework aims at allowing users to have more control, convenience and privacy over their identity and profile information. User should be able to decide what information he wants to share and with which websites. Higgins is a framework that accepts all well-known protocols to digital identities,

including WS-Trust, OpenID, SAML, XDI, LDAP, and others [21].

3.9. CardSpace (InfoCard)

The challenge is to create, use and manage the identity diversity in a meaningful way. The system CardSpace, originally called InfoCard [22], is a platform component of Microsoft.Net designed to offer users a consistent support for handling with multiple digital identities. Microsoft has documented the protocol implemented by Cardspace in the InfoCard specification. Furthermore, it is also supported in the browser Internet Explorer (since version 7.0). The Cardspace focuses on user data collections called information cards (InfoCards), presented in a software interface, named identity selector (similar to a wallet with cards identifying the user). Each InfoCard represents a different identity. When a service provider (SP) requests user credentials, the user agent picks from the selector program, one of their identities.

4. Comparison between the different AAIs

This section analyzes and compares infrastructures and technologies used for building IdM system. The idea is to compare the different infrastructures for being used in secure exchanges of identity information and for maintaining user privacy. This overview is not intended to draw up an exhaustive list of all infrastructures and products for Identity Management. The diversity of specifications and especially the terminologies used in the various infrastructures make the comparison of these IAAs very difficult.

4.1. Considerations about IdM solutions

The first step to resolve the interoperability problems is the understanding of the difference between the technologies. Some projects are developed to promote interoperability in federated systems. The Kantara Initiative [23] created an organization to address interoperability challenges which exist between companies and firms that offer web services and applications. This initiative aims to promote innovation required for broad adoption of interoperable solutions to federated identities, aligned to the needs of mobile networks. Already the Open Source Identity System workgroup [24] aims to contribute for building a layer of interoperable identities from commercial solutions and main AAIs. Current projects include efforts to promote interoperability between Information Card and AAIs.

The IdM infrastructures described in section 3 share some points in common, such as SSO, distribution of authentication procedures, attributes exchange, concerns about user privacy and anonymity. The SAML specifications present a general framework for dealing with federated identities, in which metadata are defined to represent security information, protocols for exchanging security assertions and trust relations. SAML was employed by several other IdM solutions, including frameworks presented in section 3.

There is some overlap between WS-Federation and SAML standards. Both solutions allow federated IdM and provide a similar set of features: WS-Federation provides SSO, SLO, attributes exchange (based on privacy policies), trusted relationships, permanent and transient pseudonyms and metadata documents. The main difference is that the WS-Federation is based on the trust model of WS-Trust and allows the use of any credentials, not only SAML assertions.

The Liberty Alliance project aimed to facilitate business interactions, taking advantage of Service Oriented Architecture (SOA) and the concept of federation, which is characterized by the notion of circles of trust in the specifications. One of the contributions of this project was having influenced SAML specifications, many suggestions of Liberty Alliance are now part of SAML 2.0. The Liberty Alliance project provides similar features to those of WS-Federation which is founded on a stack of all Web services specifications such as WS-Trust and WS-Policy [25]. Liberty Alliance implements an approach for sharing user attributes based on user permissions [26]. In this case, user should be placed in control of releases and uses of his personal information stored in an attribute provider or IdP. A protocol is defined for determining the message exchange necessary. The access request must specify purpose of the use or of the requested information. And, the response can determine the user preferences in terms of privacy or the policy for the required resource access.

The Shibboleth project is based on open standards, such as XML and XAML, it inherits their features and provides an easy way to enable applications to use facilities of a federated identity model. Several functionalities specified in SAML 2.0 were implemented in Shibboleth in order to provide the SSO and secure exchange of user attributes for all service providers that take part of a Shibboleth federation. The authentication of users can be done through user name and password, Kerberos, X.509, etc.

OpenID, CardSpace and Higgins are frameworks that support IdM approaches of federated identities and User-Centric controls. Among these infrastructures, the best succeeded is OpenID. It has been widely used, especially due to partnership with companies offering Web 2.0 applications. One advantage of OpenID is that it does not require software on the client side. The CardSpace and Higgins adopt the model of active client (with Identity Selector), and the active client of Higgins is available for different platforms of data representation and accepts all well-known protocols to digital identities, including WS-Trust, OpenID, SAML, XDI, LDAP, and others.

Another difference is that the OpenID approach adopts the identity model based on address. This identifier (or handle) is usually a URL (Uniform Resource Locator) or, in some cases, an XRI (Extensible Resource Identifier). Meanwhile, CardSpace and Higgins adopt identity approaches based on cards (tokens). The literature shows that Higgins approach is considered more flexible because it supports identities provided from different sources and prevents an identity provider of tracking the service providers (applications) accessed by the user. While providing support for any type of security token, the protocols adopted in CardSpace [27] only follow Web Services (WS-*) standards, focusing mainly on WS-Trust. However, project Higgins of the Eclipse Foundation follows a more independent solution, since it supports identity providers based on WS-Trust but also based on SAML 2.0.

OAuth comes from the social web, with version 1.0 (RFC 5849), it is an open protocol that supplies a standard API for user authentication in desktop and Web applications. OAuth is not an OpenID extension. The OAuth aims to

support application developers with a standard API for service providers without forcing users to expose their credentials. The main goal of OAuth is to allow an application to be authenticated to another "on behalf of a user" without needing access to his password.

The main difference between OpenID and OAuth refers to the fact that OAuth defines mechanisms for granting user accesses to resources while OpenID seeks to ensure that a user really is who it claims to represent. These two technologies can work together.

Currently, e-gov infrastructures and applications, such as those of U.S. government, begin to be based on open identity technologies (OpenID, CardSpace). SAML is considered an open identity technology, but its previous need for trust relationships between IdPs and SPs, makes this technology not scalable to Web 2.0 applications. Given this, open trust frameworks are being developed to enable the Government websites and applications to accept credentials issued by different identity providers, commercial and academic [28].

4.2. Considerations about Privacy in IAAs

Privacy is of paramount importance, the concept of federated identities gives users a convenient way to create identities and deal with various SPs. Besides to all the simplicity and convenience offered, it is necessary to take into account that federated Identity management becomes a crucial task in large systems and also the multiples threats against privacy of user data. Any infrastructure of IdM must adequately protect user information and must adhere to the privacy policies defined to the user personal data.

The sharing of user information (identity or attribute data) is also a significant challenge if user privacy is considered in federations. Also, it appears that federated identity systems are conceived for having among their main objectives the sharing of such information. Also, federated identity systems often manipulate different kinds of identifiers in different contexts. Such identifiers can have an absolute meaning (context independent) or relative (context dependent) [29]. The privacy in federations may be emphasized with minimal data disclosure. For example, authentications and authorizations can be performed with LoA and a minimal data disclosure by providing only identifiers and attributes necessary to ensure the service execution or resource accesses.

An important technique for the preservation of privacy is the use of pseudonyms, which are user identifiers that do not allow inferences regarding the real identity, properties, or attributes of users to whom they refer. Pseudonyms may have local meaning, dependent on the context between user and SP, or global, context independent and valid for the whole federation. The validity can also be temporary or permanent [29].

WS-Federation defines a Pseudonyms Service which is responsible for associating pseudonyms to user identities. In WS-Federation, pseudonym may have different levels of volatility allowing different levels of customization and privacy. For example, a subject can have pseudonyms which last only one authentication session. In addition to increase its privacy, it prevents services to associate any persistent information with the subject (preventing customization). Unlike IdP and Attribute Service, the Pseudonym Service uses a different interface not based on the STS, but defined in the WS-Transfer [30]. This specification defines methods to create, delete, update and access existing pseudonyms.

The pseudonyms which are used in SAML Assertions are built based on pseudo-random values that do not have discernible correlation with user identifiers in IdPs or SPs. A pseudonym has a meaning only in the context of the relationship between the two communicating parties. Pseudonyms are also intended to difficult the association between users and their transactions (services being accessed).

Specifications of Liberty Alliance also address issues about policies of privacy multi-level [26], which make use of privacy labels similar to privacy and security labels in Mandatory Access Control (MAC). In MAC controls, each resource is tagged with a security label that represents the sensitivity of the resource considered. A user (subject) wishing to access a resource must have an authorization level (clearance level) appropriate to the security label of the resource. In Liberty Alliance specifications, privacy levels follows the privacy policies available in the identity providers (which also serve like repositories for user attributes) and are assigned to user data and to attribute requests sent by service providers to IdPs.

Shibboleth has an emphasis on the privacy of users' attributes. The release of these attributes for service providers is conditioned by the privacy policy of the origin domain and also by user preferences. The great limitation of CardSpace and Shibboleth is that the user can select only one identity provider and submit only one credential to a service provider. For solving this problem, it is proposed a component called Linking Service [31]. The idea of this service is to allow users to add various attributes from different IdP and yet preserving the privacy of those users. The Higgins project also intends to work this problem, but the current version does not yet offer a solution.

4.3. Levels of Assurance in IdM IAAs

In OAuth or OpenId, when generating user accounts, the IdP does not have means to confirm the user's real identity. In this case, the LoA of the Identity is low (LoA = 1). OpenID is currently used mostly for low-risk applications like blogs and social networking, not commerce, education, or government [32].

The SAML used in many infrastructures for IdM, allows to associate quality levels to its authentication assertions, providing, in this way, a standard way to define levels of information exchange between IdP and SP. Therefore, LoA levels can be included using an Authentication Context (AuthnContext) mechanisms [33]. The AuthnContext is a new specification defined in SAML 2.0 for providing a simplified way of representing a LOA authentication scheme and to enable the authentication service to include some information related to the quality of the authentication process.

According to the E-Authentication Federation rules (EAF) [34], the LoA value is a compulsory attribute that must be present whenever a SAML authentication assertion is issued. The EAF has defined a special URI : (us:gov:eauthentication:basic:assuranceLevel) to uniquely

identify the LoA attributes, and the attribute can only have values of 1, 2, 3, 4 or "test".

Like SAML, Liberty Alliance formed the Identity Assurance Expert Group (IAEG). The IAEG's objective is to create a framework of baseline policies, business rules, and commercial terms against which identity providers can be assessed and evaluated. The primary deliverable of IAEG is the Liberty Identity Assurance Framework (LIAF) [35][36]. Which goal is to facilitate identity federation to promote uniformity and interoperability amongst identity providers, with a specific focus on the level of trust (LoT), or LoA, associated with identity assertions.

WS-Trust specification defines the AuthenticationType parameter to indicate an authentication type that is required (or performed) with respect to a particular security token request. However, no specific recommendations regarding mechanism or LoA and no particular types are defined or required. To facilitate interoperability WS-Federation has identified and defined a set of Universal Resource Identifiers (URIs) for specifying common authentication types and assurance levels that can be used for the wst:AuthenticationType parameter in RST and RSTR messages.

CardSpace and Higgins are two Identity Metasystems, entirely agnostic about the format of the security token that's requested from an IdP and passed on to a SP, which define a similar mechanism to allow service providers to specify the authentication requirements of the services they offer. Both identity systems are built around the abstraction of the information card, which is a standard representation of the user information. In fact, CardSpace and Higgins typically aren't even aware of what format is in this token. Because of this, these systems can work with any digital identity system, using any type of security token, including simple usernames, X.509 certificates, Kerberos tickets, SAML tokens, or anything else.

Basically, in these systems, when the user tries to access some service, the information card client installed in his device recovers the SP policy to determine the requirements of the service. The user selects one of the cards satisfying the policy requirements; the information card application contacts the IdP that issued that card to get a signed token. Finally, this signed token is sent to the SP for authorizing access to the aimed service. The required LoA for getting access to the service depends on the SP policy and the authentication requirements defined for this service. The use of the SP policy in these systems provides the same assurance level that is described in SAML or Liberty Alliance infrastructures.

5. Final Considerations

Cloud Computing, collaborative networks, mobile Computing and other new applications and computing models are offering new possibilities of connections. However, the way people and organizations (private and public) will make use of these opportunities and applications will depend on the progress of digital identity authentication and Identity Management system [37]. As seen in this text, federated identity and User-Centric models, when applied in Identity Management systems, bring benefits to both, users and service providers. It is noted that promote federated identity, also presents complex challenges in terms of technical issues and human needs.

The main frameworks and models to IdM were described and analyzed in this text. It was indicated the importance of SAML 2.0 which is the basis for many of these frameworks. Shibboleth has become a "de facto" standard in academic networks and the solution Liberty Alliance is being adopted by a large community of private and public companies. The latest solutions have also emphasized User-Centric models. OpenID and CardSpace in particular has attracted a lot of interest, especially of service providers that follow Web 2.0 approach and by governments who wish to actively include people in their social networks and E-Gov programs.

The use of the infrastructures for identity management can be a deterrent, analyzing costs vs. benefits. Even on the assumption that the trusts relationships are already pre-established among the different administrative domains that represent a federation. Yet there are several challenges to implement authentication credentials on a federation. Service providers and domains have the autonomy to decide which policies and security technologies they want to use, i.e., a federation needs to provide an infrastructure that supports SSO authentication even with partners that use different security credentials. The interoperability provided by WS-Trust specification and SAML standard may solve the great part of the problems but it is not evident that can solve all problems of credentials transposition between domains of a federation.

Interoperability is an ongoing challenge for developing federated identity [12]. However, many developers are having success in combining different solutions, to then access a service.

6. Conclusion and choices in SecFuNet Infrastructure

Federated IdM is a topic of active research and, probably, given the complexity and relevance, will therefore continue for many more years. This conclusion stems from the numerous questions and issues which systems of federated identities should consider. Features like ease of use, user privacy and anonymity, strong security, single authentication on different technologies, scalability, access control mechanisms of thin granularity (attribute-based controls) and customized services are suitable in new distributed applications.

Through our investigation, we identified a significant interest across various communities, in using levels of authentication assurance as a qualifier of the strength of an authentication process. We have found large interest in LoA definitions, and in finding out how LoA may be used to achieve fine-grained access control of sensitive resources. This may enable service providers to make their access control decisions based on the LoT and to link the LoA with authorization decisions, helping to mitigate risks and provide more secure and fine-grained access control.

SAML based infrastructures (Shibboleth and Liberty Alliance) are strong candidates to be adopted for identiy management in the context of SecFuNet project. Such tools use well-defined identity models and they present several interesting features for SecFuNet, like advanced privacy mechanisms, with a specific focus on LoA. The interoperability guaranteed by the use of SAML is effective

and well accepted. SAML assertions allow the use of many different authentication technologies, making these frameworks very interesting for heterogeneous environments. However, despite the indicated advantages, there are limitations in order to fulfill the SecFuNet requirements. In particular, the support for SmartCards is either limited or non-existent and even I-Cards are not an option. Besides, these infrastructures are based in complex protocols that require the inclusion of large implementation stacks in clients limiting the utilization of these infrastructures in mobile devices.

In this overview, we concluded that the most effective platform to fulfill, at least in part, the SecFuNet requirements is OpenID. Despite the gap in supporting LoA and privacy protection, protocols for authentication and attribute exchanges are extremely simple in this infrastructure and in this way, allowing the integration in a wider variety of applications and devices. OpenID may be used with any kind of authentication technology and it is important to the SecFuNet infrastructure. With respect to attribute management, it is possible to use any type of policy, including User-Centric management. User-Centric IdM is intended to be applied in the SecFuNet. We are planning to introduce smart cards and user controls in attributes' delivery in the OpenId. Also, we are extending this infrastructure for supporting authentication mechanisms based on LoA levels.

References:

[1]:http://www.secfunet.eu/repo/Public%20Deliverables/Secfunet_D3_1_v4.pdf

[2]: Clauß, S. and Köhntopp, M. (2001). Identity management and its support of multilateral security. Computer Networks, 37 (2):205–219.

[3]: Chadwick, D. (2009). Federated identity management. Foundations of Security Analysis and Design V, pages 96–120

[4]: Bhargav-Spantzel, A., Camenisch, J., Gross, T., and Sommer, D. (2007). User centricity: a taxonomy and open issues. Journal of Computer Security, 15(5):493–527.

[5]: Jøsang, A., Fabre, J., Hay, B., Dalziel, J., and Pope, S. (2005). Trust requirements in identity management. In CRPIT '44: Proceedings of the 2005 Australasian workshop on Grid computing and e-research, pages 99–108, Darlinghurst, Australia. Australian Computer Society, Inc.

[6]: Maliki, T. E. and Seigneur, J.-M. (2007). A survey of user-centric identity management technologies. In The International Conference on Emerging Security Information, Systems, and Technologies, 2007. SecureWare 2007, pages 12–17.

[7]: Camenisch, J. and Pfitzmann, B. (2007). Security, Privacy, and Trust in Modern Data Management, chapter Federated Identity Management, pages 213–238. Springer Verlag.

[8]: Damiani, E., di Vimercati, S. D. C., and Samarati, P. (2003). Managing multiple and dependable identities. In IEEE Internet Computing, pages 29–37. IEEE.

[9]: Burr, W. E., Dodson, D. F., and Polk, W. T. (2006). Electronic authentication guideline. NIST Special Publication, 800:63. http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[10]: OASIS (2005g). Security Assertion Markup Language (SAML) 2.0 Technical Overview. OASIS.

[11]: OASIS (2005a). Assertions and Protocols for the SAML 2.0. OASIS.

[12]: Maler, E. and Reed, D. (2008). The venn of identity: Options and issues in federated IdM. Security Privacy, IEEE, 6 (2):16–23.

[13]: OASIS (2005b). Bindings for the OASIS SAML V2.0. Organization for the Advancement of Structured Information Standards (OASIS).

[14]: OASIS (2009b). WS-Trust 1.4. http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/ws-trust-1.4-spec-os.html

[15]: W3C (2007). Web Services Policy 1.5 - Framework. http://www.w3.org/TR/2007/REC-ws-policy-20070904.

[16]: OASIS (2009c). Web Services Federation Language (WS-Federation) Version 1.2. http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html

[17]: Scavo, T. and Cantor, S. (2005). Shibboleth Architecture, http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-tech-overview-latest.pdf.

[18]: Liberty (2003). Introduction to the Liberty Alliance Identity Architecture,http://xml.coverpages.org/LibertyAllianceArchitecture200303.pdf.

[19]: Baldoni, R. (2010). Federated Identity Management Systems in e-Government: the Case of Italy. Electronic Government: An International Journal, 8(1).

[20]: http://www.xfront.com/REST-Web-Services.html

[21]: EclipseFoundation (2010). Higgins open source identity framework, http://www.eclipse.org/higgins/.

[22]: http://msdn.microsoft.com/fr-fr/magazine/cc163434.aspx].

[23]: http://kantarainitiative.org/

[24] http://osis.idcommons.net/wiki/Main_Page

[25]: Kallela, J. (2008). Federated identity management solutions. Technical report, Helsinki University of Technology.http://www.cse.tkk.fi/en/publications/B/1/papers/Kallela_final.pdf.

[26]: Aarts, R. and Madsen, P. (2006). Liberty ID-WSF Interaction Service Specification v.2.Liberty Alliance Project. http://www.projectliberty.org/liberty/content/download/.

[27]: Chappell, D. (2006). Introducing windows cardspace. MSDN technical articles, Microsoft Corporation. http://msdn.microsoft.com/en-us/library/aa480189.aspx.

[28]: Thibeau, D. and Reed, D. (2009). Open trust frameworks for open government: Enabling citizen involvement through open identity technologies. White paper, OpenID Foudation and Information Card Foudation.

[29]: Ahn, G.-J. and Lam, J. (2005). Managing privacy preferences for federated identity management. In DIM '05: Proceedings of the 2005 workshop on Digital identity management, pages 28–36, New York, NY, USA. ACM.

[30]: W3C (2010). Web Services Transfer (WS-Transfer). http://www.w3.org/TR/2010/WD-ws-transfer-20100805.

[31]: Chadwick, D. and Inman, G. (2009). Attribute aggregation in federated identity. IEEE Computer, pages 44–53.

[32]: http://csrc.nist.gov/publications/nistir/ir7427/NISTIR7427_PKI_2007.pdf

[33]:https://www.oasis-open.org/committees/download.php/32483/sstc-saml-loa-authncontext-profile-draft-diff-03.pdf

[34]: US Government's 'E-Authentication' Federation, http://www.cio.gov/eauthentication/

[35]:http://www.projectliberty.org/content/download/4315/28869/file/liberty-identity-assurance-framework-v1.1.pdf

[36]: The ES-LoA Project WP1 Deliverable "Using LoA to Achieve Risk Based Access Control", A Study Report May 2007 Aleksandra Nenadić and Ning Zhang School of Computer Science University of Manchester

[37]: Lewis, J. A. (2008). Authentication 2.0 - new opportunities for online identification. Technical report, Center for Strategic and International Studies.