

Enabling User Control with Personal Identity Management

Ty Mey Eap, Marek Hatala
*School of Interactive Arts and Technology,
Simon Fraser University, Canada
teap, mhatala@sfu.ca*

Dragan Gašević
*School of Computing and Information Systems,
Athabasca University, Canada
E-mail: dgasevic@acm.org*

Abstract

Being proactive and vigilant is the best defense against identity theft and the invasion of privacy. This recurrent advice from the public broadcasting attests that security breaches can happen and no identity management system can provide full-proof security. The challenge is even greater in service-oriented architectures where each user has their identities scattered across many services and has no control over management of those identities. Recent research in the area of the user-centric identity management makes user control and consent the key concept for identity management, but there is no consensus on the level of user-centricity. This paper proposes a service-oriented architecture framework called personal identity management that truly puts users in control over the management of their identities. The advantages of this proposal can be demonstrated through a comparison analysis of relevant identity management systems against a set of criteria required for today's identity management.

1. Introduction

The advice from authorities such as Canadian Federal-Provincial-Territorial Consumer Measures Committee or US Federal Trade Commission and from mass media is to be proactive in the fight against identity theft and fraud—people should shred their personal documents before disposing them and regularly check their financial statements. However, it is difficult for a user to be proactive in today's "domain-centric" identity management (IM) [2, 13]. Treated as "dummy" end-users, users have no control and usually become aware of a security breach after their accounts have been affected or cancelled. As the number of online services grows, users have their identities scattered across multiple systems and services. As a result, domain-centric IM can no longer handle today's IM requirements. This forces researchers to consider fundamental changes in the IM [13] and believe the answer is in the user-centric IM. This new IM paradigm shifts the focus towards users and provides stronger user control [2, 6, 13, 19]. However, there is no universal set of criteria for user-centricity, which can affect the research on user-centric IM [2, 6, 13].

In this paper, we define user control and consent as the ability for users to have the last words for the release of

their identity data and the ability to inspect all the consents they have made—being proactive. An IM system should provide tools to assist users in their tasks to ease the adoption of the new IM practices (i.e., shifting from being passive to being proactive). These goals are achievable if each user has a personal identity provider. Based on this premise, we propose a personal identity management (PIM) framework, a service oriented architecture framework that gives users full control over the management of their identity data, reduces the complexity of the trust and privacy management, and strengthens the Internet and Web service security. These advantages can be seen through the PIM framework analysis and the comparison analysis of relevant IM systems against a set of criteria required for today's IM and used for the design of the PIM framework.

2. Personal Identity Management (PIM)

Before discussing the PIM framework, we first clarify some definitions and define relevant parameters. Next, we explain the concept of personal identity provider and design goals of the PIM framework. These definitions and the design goals allow readers to understand our vision of an IM system and therefore, the PIM framework.

2.1. Definitions

What is an IM? Wikipedia defines digital IM as a management of user credentials and user accesses to an online system. **Authentication** is an integral part of the IM; it serves to verify about specific identity claims. Therefore, it is fundamental to include other security constructs such as authentication, authorization and access control when discussing an IM system [12]. An **identity** is a person's self-affiliation as a member of a group or an organization.

Identity Provider (IdP). In this paper, we define an IdP as a trusted entity that can verify the authenticity of a user during registration, has the authority to issue sets of credentials, is able to authenticate users, and finally provides IM services to a relying-party.

Relying-party (RP). An RP is a service provider that relies on a third party IdP for its IM. An RP may or may not have registered users. An RP that has registered users is a home-based RP for those users.

Single sign-on (SSO). A widely accepted definition, SSO is an authentication system that enables a user to

authenticate once and then gain access to the resources of multiple software systems.

User Profile. Also known as a persona, a user profile is a set of identity data. A user can have more than one profile, and each profile identifies a user in a particular context.

Security is generally understood as the prevention of spying, attacks, or theft [21]. Preventing identity theft is a main concern in this paper, which involves stealing or hijacking the identity of another person and using it to commit crimes against or in the name of that person.

Privacy is an ability to keep personal affairs out of the public view. Protecting privacy is a collaborative effort. The society as a whole must practice and obey privacy regulations. RPs must safeguard user information and not release it without user authorization. The security infrastructure must find ways to reduce the risk of data collection that can be used to determine user habits or behaviors. In the absence of trust, anonymity should be used to prevent the data collection.

Add-on is a software component attached to Web browsers that can intercept and preprocess HTML stream (e.g., InfoCard add-on [5], Sxipper [10], etc).

2.2. Key Concepts and Design Goals

The concept of a personal IdP simplifies the design of the IM framework and allows users to manage their own identities and be the watchdogs of their personal security. Moreover, it breaks down the responsibility for the security and privacy protection and makes them easier to manage. Since users are responsible for their security and privacy, an RP only has to focus on the security of the resources and accessing policies. With the help of trusted personal IdPs, an RP can trust users to be authentic while users can determine if they should trust an RP to be legitimate. This change in the concept of trust enables an RP to be independent and to establish its own trust and security policies.

2.2.1 Personal identity provider (PIpP)

A PIpP has some similarity to a home-site in terms of Sxip or OpenID [18]. It provides storage for identity data and assists users in the management of their identities. Its functions include:

1. Provide a smart and strong authentication service to users with different levels of security (e.g., a user may use a set of credentials that has security level 1 to access her blog or a chat room, a second set of credentials with security level 2 to access academic computing services, a third set of credentials with security level 3 to access online financial services, and so on);
2. Allow a user to consent or confirm that she is the person who is attempting to access resources of an RP that requests authentication confirmation from the user's PIpP;

3. Manage user profiles;
4. Allow users to access their profiles using different sets of credentials with different levels of security;
5. Manage signed affiliation-claims for each user;
6. Log all transactions and make them transparent to users;
7. Detect anomalies and alert users of a possible security risk; and
8. Build a body of knowledge of RP reputations to advise users on the security risks.

2.2.2 Simplifying trust policy

Trust is the root for all security stands. Currently, to provide a SSO solution across multiple organizations, a trust federation is a common approach (e.g., Shibboleth [17] and Liberty Alliance [15]). However, building trust policies for a federation involves a lengthy negotiation. A federation must have a well-written trust policy agreement among IdPs and RPs. In his keynote speech, Sixp CEO, Dick Hardt, implies that in the real life, due to its complexity a federated trust is difficult to achieve [10]. In summary, building a trust federation of a similar type of organizations is feasible, but building a trust federation for organizations that need different levels of security is a challenge.

With PIpP, trust policies are easier to design since each RP is independent and can build its own trust and security policies. The policies can be a combination of both user reputation-based trust policy and RP agreement policy. A trust policy based on users' reputation is complex and depends on the RP's security levels. It shall be used as additional information for making authorization decisions. We leave the discussion of reputation-based trust policy for our next research.

For RP agreement policy, PIM adopts a distributed trust model. An RP can create a trust policy that accepts a remote user who presents an affiliation-claim signed by a trusted RP and her PIpP. An affiliation-claim can be a digital certificate or a SAML assertion [1].

2.2.3 Simplifying security protocols

The PIM framework has three basic protocols:

1. A protocol for an RP to get user consent proofs or affiliation-claims from a PIpP;
2. A protocol for a PIpP to get and affiliation-claims from an RP for a user; and
3. A protocol for PIpP to release a user profile to an RP.

These protocols should be simple and use existing open standards when it is possible. Finally, a user ID could be as simple as an email (e.g. john@pip.bc.ca), which has an identifier and a URL to a PIpP.

2.2.4 User consent

User consent is a concept that can render identity data useless to thieves. Traditionally, IdPs and RPs require users to authenticate in order to gain accesses to a system.

In the PIM framework, users must consent to authentication confirmation from an RP. When a PIdP asks a user for the consent, it displays the purpose of that consent and logs the transaction, so that the user can verify it later. A close relationship between a PIdP and the user makes impersonation impossible. A PIdP can detect anomalies and can warn users about security risks. An example of an anomaly is an access attempt that does not follow a regular established access pattern.

2.2.5 Integration and Scalability

PIM complies with existing standards and uses technologies developed by existing IM solutions. This should guarantee easy integration of the PIM framework with existing IMs. Shibboleth [17] and Liberty Alliance [15] can use PIM with a simple modification. Instead of asking users where they come from, these systems would ask users to enter their personal ID. From the ID, the systems can determine where the users come from and continue with its processes. Similarly, scalability is not an issue for PIM. It only requires each user using a PIdP, but an RP can accept multiple PIdPs. Local organizations can provide PIdP services to local users. Such practice would strengthen security and improve efficiency.

2.3. Security and Privacy Concerns

How secure should a PIdP be? PIdP is a point of control and functions as a user's assistant. It can act on user's behalf to release preauthorized consents and the user's identity data. It learns authentication and accessing patterns, detects anomalies, and alerts users if there is an access attempt that does not fit an established pattern. Therefore, a PIdP must be a trusted entity, follow best security practices, and obey the privacy laws. At the same time, the risk of privacy violation is minimal. A PIdP only holds the user identity data and a list of RPs the user had accessed. Although this information may be useful to a marketing firm, there are easier and legal ways for a marketing firm to obtain such information. Therefore, the risk is manageable.

Can PIM support anonymity? Because in some cases anonymity can be useful, the PIM framework supports anonymity with the use of anonymous affiliation-claims. However, anonymity is a double-edged sword. On one hand, it provides some privacy protection to users, but on the other hand, it increases security risk [8, 9]. It allows malicious users to violate trust and privacy of other users without being caught. In addition, for an anonymous algorithm to be effective, it must be supported by the use of a proxy or a network protocol that hides the users' IP addresses [14]. Otherwise, it is possible to correlate two anonymous accesses to the same user.

2.4. An Overview of the PIM Framework

To ease the understanding of concepts and ideas of the PIM framework, we describe it in term of scenarios. Note

that PIM is built on a service-oriented architecture (SOA). Requests to a PIM component (e.g., PIdP, add-on, and RPs) are supported by Web services, but for simplicity, we omit this detail in the descriptions of the scenarios. The first scenario describes a registration process to an RP. Through this process, a user verifies the security mechanism while the RP verifies the user's PIdP. Once registered, the user becomes a member of the RP, and the RP becomes the user's home-based RP and can sign the user's affiliation claims. In the second scenario, we describe the authentication confirmation process when a user attempts to access resources on a home-based RP. This scenario is also similar to the use of a signed affiliation claim to access resources on a remote RP, which is described in the third scenario. The fourth scenario is the use of the PIM framework in a secure electronic payment. This scenario demonstrates that it will be difficult for a thief to use a stolen credit card in the PIM framework.

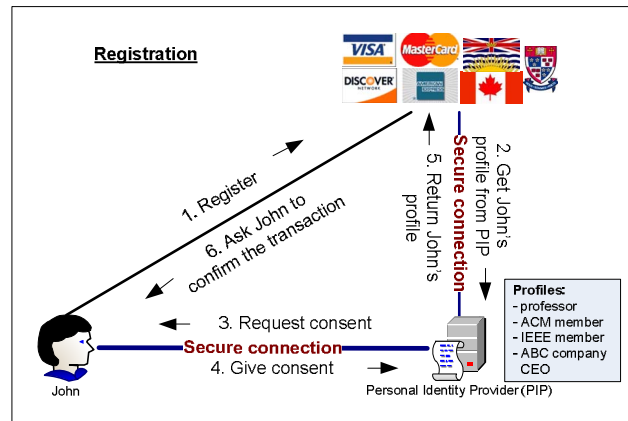


Figure 2.1 Register to a RP

Scenario 1: In Figure 2.1, to register to an RP, John types in his ID into the RP registration form (e.g., bigjohn@pip.bc.ca). Since the ID is a combination of an identifier and a URL to John's PIdP, the RP is able to request his profile from the PIdP. John can create a new ID that matches the security level required by the RP. John's PIdP prepares the registration form using identity data it has and asks John to modify and/or fill in the missing information. Once registered, the RP becomes John's home-based RP and can certify its affiliation with John to allow John to access resources on a partner RP. John can register to as many RPs as he wants. We are building a PIM add-on similar to Skipper [10] or InfoCard [5] to help John securely login to his PIdP, intercept login forms, and automatically fill in appropriate John ID with respect to a home-based RP.

Scenario 2: In Figure 2.2, when John accesses resources on a home-based RP site, the RP requests John's PIdP for a proof of John's consent. The process is as follows. The RP responds to John with a login page that has a special tag in the HTTP header. If John uses a PIM add-on, it automatically captures the login page and

his credit card. This payment process is similar to an electronic wallet but much safer.

These four scenarios show that the proposed PIM can enhance security and give users full control over the release of their private information via the consent mechanism. The framework is transparent to the users and makes users a participant of the IM system. The ability to get user consent allows PIM to deal with special needs for the release of personal information. For example, rules, laws, and regulations can be written into the PIDP policies to allow the PIDP to release the user's personal information in the case of an emergency. If a search and rescue team needs to know a user's blood type or the user's last seen location, the PIDP can be authorized to release this information on behalf of a user.

3. Analysis

This section discusses the current state of the IM. We begin with the domain-centric IM, which is a dominant type of IM in the industry. Domain-centric IM systems are suitable for independent systems, but it cannot support the IM requirements of collaborative and service-oriented systems. The emerging user-centric IM has the potential to meet the requirements of today's IM. The following analysis will show how PIM captures this potential.

3.1. What do we look for in an IM system?

Cameron's Seven Laws of identity [3] are a good starting point for building our analysis criteria. The laws discuss common issues regarding today's IM and has spurred some good exchanges of ideas between Cameron and Sxip CEO, Dick Hardt, on Cameron's Identity Weblog (<http://www.identityblog.com>).

Law 1: User Control and Consent. *The system must put users in control of what digital identities are used and released, protect users against deception, and verify the identity of any party who asks for user information.* This law is essential for today's IM [3, 19]. In the introduction, we gave our definition of *user control and consent*; users must know what they consent to and be able to view what they had consented.

Law 2: Minimal Disclosure. *Since security breach can happen, the IM system should limit the disclosure of identity information for a constraint use.* The domain-centric IM research strongly supports this view. For example, the use of anonymous access is an attempt to prevent the correlation of IDs [2, 4, 7]. This law becomes less relevant if users are in control of their identity data. However, *anonymity* can be also useful in some cases.

Law 3: Justifiable Parties. *An IM system must only disclose identity information to parties having a necessary and justifiable place in a given identity relationship.* Cameron's position is vague on this law. He does not want to get involved in the fabric of trust. Instead, he simply suggests that users should determine whom they can trust, and the IM system should provide

the necessary information for the users to make these decisions (e.g., InfoCard alerts users and gives the RP information when users access an RP site for the first time). We consider this law as allowing *users to decide whom they should trust*.

Law 4: Directed Identity. *An IM system must support both omni-directional (public) identity to facilitate the discovery and unidirectional (private) identity to prevent unnecessary release of correlation identity information.* In the real world, people need to know with whom they are dealing with, which should not be different on the Internet. This view echoes in Dick Hardt's slogan "Who Is the Dick on My Site?" However, accountability is not Cameron's view of a public identity. His view is a generic identity for accessing some services on a public domain, and therefore, there is a need for private identity. Since RPs have different levels of security, supporting *multiple IDs* is essentials in a modern IM system, which is the same for the *identity discovery*.

Law 5: Pluralism of Operators and Technologies. *The IM system should be able to work with multiple IdPs.* Obviously, for scalability, the IM framework must continue to support *multiple IdPs*, but it does not mean that a user must have more than one IdP. This paper has shown that a PIDP makes the IM framework design simpler and provides a stronger security.

Law 6: Human Integration. *The IM system must define the human user to be a component of the distributed system integrated through unambiguous human/machine communication mechanisms.* User centric IM and, in particular, PIM strongly support this view. User participation is central to the PIM framework design, and this design principle is reflected in the user control and consent of an IM system.

Law 7: Consistent Experience across Contexts. *The IM system must provide users with a simple and consistent experience while enabling separation of contexts through multiple operators and technologies.* By definition, SSO provides consistent user experience across multiple contexts. Users authenticate to an IdP and are able to access resources on different service providers.

3.2. Domain-Centric Identity Management

To eliminate risks of the privacy violation, domain-centric IM systems are designed as well-protected silo systems, so that the sharing of user information, intentionally or unintentionally, is not possible. Traditionally, each service provider has their own IM system. Even in the same organization, a user may be asked to login multiple times because each service provider needs to verify the authenticity of the user. In today's service-oriented computing world, it is common that businesses and organizations share their resources with each other. Consequently, federated IM was introduced as a solution to enable the sharing of the resources across multiple organizations. This section

analyzes three well-known domain-centric IM systems: Kerberos [4], central authentication system (CAS) (<http://www.ja-sig.org/products/cas/>), and Shibboleth [17]. The analysis will show that they do not meet the requirement of the today's IM.

Kerberos is an authentication system that allows a user logged in to her terminals to access resources and services on the network of her organization [4]. When a user logs in to her terminal, Kerberos client authenticates the user to a Kerberos server, a trusted third party, known as key distribution center (KDC). KDC has two components: an authentication server (AS) and a ticket granting service (TGS). If verified, AS issues a "ticket granting ticket" and a session key for the Kerberos client. As the name suggests, the ticket allows Kerberos client to request tickets for the user to access any service on the network. Kerberos is mainly for a private network, since the ticket is granted for a specific service. Hence, KDC must be aware of the existence of that service.

CAS, designed mainly for Web applications, provides a central authentication service for different RPs. When a user tries to access a member RP for the first time, the RP redirect the user to CAS for authentication. If the authentication is successful, CAS redirects the user back to the RP with a ticket that the RP must validate before granting access to the user. CAS is not really a SSO. Users still need to login multiple times since each new RP needs a new CAS ticket. However, CAS does help eliminate the replications of identity data across the network.

Shibboleth is a "Web SSO" and is a federated IM system. It enables a user to authenticate to her IdP and access resources within a trust federation [17]. Shibboleth works similarly to CAS, but it also supports the concept of a trust federation. Like CAS, it is not a true SSO. When a user comes in to an RP site, the RP asks where she comes from and redirects the user to her IdP to be authenticated. If successful, the IdP redirects the user back to the RP with a SAML token in the HTTP header. The RP can use the token to request the user's attributes. The token contains an encrypted random number (cryptohandler) that allows the RP to get the user's attributes such as the user's affiliation or nickname, according to the policy of the federation, while it allows the user to remain anonymous.

User control and consent do not exist in domain-centric IM systems. This is the case for the three IM systems above. On the other hand, anonymity in domain-centric is the key idea for limiting the disclosure of identity information. Apart from SSO and federated IM supported by Shibboleth, the three IM systems cannot support the criteria that are essential for today's IM (See a summary of the comparison in Table 3.1 below).

Table 3.1 Domain-Centric IM Features
(- not supported, ? unsure, and √ supported)

Description	Kerberos	Shibboleth	CAS
User control and consent	-	-	-
Anonymity	√	√	?
Reputation/accountability	-	-	-
User trust making decision	-	-	-
Identity discovery	-	-	-
Multiple IDs	-	-	-
SSO	√	?	?
Multiple IdPs	-	√	?

3.3. User-Centric Identity Management

User-centric IM shifts the control of the IM from the institutions to users, giving the users greater flexibility in how and where they store their identities, gives them control over sharing and using of those identities, and provides them with stronger assurances for privacy [13]. A few systems are striving to support this idea. However, since there is no universal set of criteria to measure 'user centricity' of a system, there is a wide range of user-centric IM approaches [2, 6, 13]. In this section, we discuss a few recently emerged user-centric IM systems and see how they stand up with our selected criteria.

Microsoft claims that **InfoCard** strengthens security and privacy on the Internet [11]. InfoCard uses Cameron's seven laws of identity as its design principles. It is an interoperable architecture designed to allow Internet users to use context-specific identities from different IdPs in various online interactions [11]. When a user accesses an InfoCard compliant site, the site returns a login page that has an InfoCard tag. This tag enables the InfoCard add-on to intercept and pop up a visual "Information Card" (law 7) and ask users to select an appropriate identity for the RP site (law 1). If the RP is not in the list of visited sites, InfoCard displays a warning including the information it knows about the RP. The user has a choice to decline or trust the site (law 3).

What does InfoCard offer? Users can configure all their sets of credentials into the InfoCard system and use them without having to reenter them. However, it is not true that users can select any set of credentials. The credentials must be the one required by the RP that the users are trying to access. Hence, users must know which sets of credentials they can use, and they still have to remember all their credentials if they want to reconfigure the InfoCard system such as switching to another desktop. Users may have to use the old habit—writing the usernames and passwords on a piece of paper. InfoCard does not propose any change to the existing IM framework and hence, cannot offer strong user control.

OpenID [18], Lightweight Identity (LID), and Sxip [10] use Yadis protocol [16]. Yadis is a service discovery system that allows RPs to determine, without end-user intervention, the most appropriate protocol to use and to

authenticate a user based on a given Yadis ID. The ID can be a URL or any other identifier, such as an OASIS Extensible Resource Identifier (XRI), that can resolve the ID to a URL [14]. When a user accesses a Yadis compliant site, the site asks her to enter her Yadis ID. The site should be able to resolve the user's IdP and redirect the user to the IdP site for authentication. Once authenticated, the IdP returns the user back to the RP site. We omit security detail in this discussion because at this point, it is not relevant, and currently, OpenID, LID, and Sxip are still under development. Many of the security issues are still unresolved.

OpenID puts the Yadis protocol on the Internet map. In 2006, OpenID introduced authentication2.0 to make OpenID compliant to Cameron's fifth law of identity (the law of directed identity). It allows a user to use private digital addresses for different RPs [19]. A digital address is basically a new ID that the user can associate to one of her profiles. Recently, VeriSign had launched a Personal IdP service to the public (<http://pip.verisignlabs.com/>) free of charge. A user can create her OpenID on VeriSign IdP and use the ID on any OpenID compliant sites. Also in 2006, the Sxip company proposed *Identity2.0* [10], a framework that describes the concept of an ID that can be trusted and used anywhere. Identity2.0 strongly supports OpenID. Skipper is an Sxip's Firefox add-on that allows a user to log in using a username or an Identity 2.0 authentication mechanism such as OpenID and manages her identities and profiles. Sxip envisions the Identity2.0 as a standard identity system that can identify unambiguously who a user is on the Internet. As an ex-leader of anti-spam software developers, Hardt, Sxip CEO, recognized the needs for an intrinsic identity mechanism.

Liberty Alliance, for short Liberty, is a consortium of hundreds of organizations working towards developing an open standard for a distributed federated IM framework [15]. Recently, seven companies had passed Liberty's latest round of conformance tests for interoperability of the Identity Web Services Framework 2.0 [20]. The specifications include Liberty People Service and an open Web services framework intended for managing applications such as calendars, blogs, or photo sharing. As a user, Joe uses his company XYZ IdP in his office and uses a mobile AntarctiCom IdP when he is not in his office. However, because AntarctiCom and XYZ have an agreement with each other for the ID correlation, Joe can authenticate to either IdP and is able to access RPs trusted by either IdP. Liberty also allows Joe to share his identity data registered at an RP (e.g., Amazon) with another RP (e.g., eBay). This allows Liberty to claim that it has built-in user consent and privacy features, which is a concept for a user-centric IM.

Having the ability to choose an identity to present to an RP is only a first step. In our definition, the management of identities must be transparent to users. In Table 3.2

there is a question mark regarding the user control and consent for the discussed IM systems. When deciding what RPs can be trusted, Liberty leaves it in the hand of the IdP. In contrast, InfoCard allows users to make the decision. By using OpenID, Sxip has mechanism for the identity discovery. For Liberty, if two IdPs have an agreement for the identity correlation, then one IdP can discover an identity of a user using the ID from another IdP. Finally, we can say that all the discussed IM systems support the use of multiple identities and SSO. The summary of the analysis is shown in Table 3.2 below.

Table 3.2 User-Centric IM Features
(- not supported, ? unsure and √ supported)

Description	InfoCard	Sxip	Liberty
User control and consent	?	?	?
Anonymity	-	-	-
Reputation/accountability	-	√	-
User trust making decision	√	-	?
Identity discovery	-	√	?
Multiple IDs	√	√	√
SSO	√	√	√
Multiple IdPs	-	-	?

4. Discussion

The Liberty framework has a strong domain centric legacy. Institutions still make most of the decisions. An IdP must have an agreement with another IdP in order for them to discover user's identity in another IdP. In contrast, Shibboleth is a centralized IM. A user has her own IdP and uses an anonymous identity to access resources on any RP in the federation. Therefore, to build a trust federation, all parties in the federation must agree on the access rights, trust, and security policies.

Instead of attempting to change the IM infrastructure, InfoCard provides a tool for a user to deal with multiple sets of identity data. InfoCard is constrained by the domain-centric IM; it cannot provide a strong user control. Sxip has some similarities to the PIM framework. However, the flow of user control and consent of Sxip is different, and the consent is not as transparent as in the PIM framework. In addition, both have different objectives. Sxip aims to provide an IM system that can identify unambiguously users on the Internet. PIM looks for an IM solution that puts users in control of their identities, provides strong and personalized security for each user, and enables identity management in a collaborative system such as a service-oriented architecture.

5. Conclusions and Future Research

In this paper, we have shown that personal identity management framework can respond to the challenge of today's identity management. Its application is imminent as computer systems move towards service-oriented

architectures. In a collaborative environment, having multiple identities and authentication systems makes security configuration too complex and unfeasible. By complying with existing standards and using existing technologies, we increase PIM interoperability. Existing identity managements should not have any problem integrating PIM as parts of their solutions.

Our proposed framework elevates relying-parties' responsibility from monitoring users' security. This idea simplifies the design of security policies. Each relying-party negotiates and builds its trust and security policies independently. Circles of trust can be created dynamically, and institutions can share resources without going through complex security settings. Through the four scenarios, we had demonstrated that personal identity management framework could be implemented with existing security technologies, and PIM communication protocols can be supported with current open standard protocols such as SAML and Web service security standards.

Currently we are building a prototype of the proposed framework, and we plan to test it with a real system. This implementation will allow us to layout some groundwork for future research including releasing user identity data in emergency situations and resolving security issues in service-oriented architectures. Another important area of our research is trust management and access control policies. With the user consent, an RP would be allowed to collect data for a reputation-based trust policy and allow users to use their reputations to gain access to other systems.

6. References

- [1] "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0," [Jan 31, 2007]. Available: <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- [2] A. Bhargav-Spantzely, J. Camenisch, T. Gross and D. Sommer, "User centricity: A taxonomy and open issues," in *DIM '06: Proceedings of the Second ACM Workshop on Digital Identity Management*, 2006, pp. 1-10.
- [3] K. Cameron, "The laws of identity," Microsoft Corporation, May 2005, 2005.
- [4] I. Cervesato, A. D. Jaggard, A. Scedrov and C. Walstad, "Specifying kerberos 5 cross-realm authentication," in *WITS '05: Proceedings of the 2005 Workshop on Issues in the Theory of Security*, 2005, pp. 12-26.
- [5] D. Chappell, "Introducing windows CardSpace," Microsoft Corporation, Apr. 2006, 2006.
- [6] S. Clauß, d. Kesdogan and T. Kölsch, "Privacy enhancing identity management: Protection against re-identification and profiling," in *DIM '05: Proceedings of the 2005 Workshop on Digital Identity Management*, 2005, pp. 84-93.
- [7] S. Clauß and S. Schiffner, "Structuring anonymity metrics," in *DIM '06: Proceedings of the Second ACM Workshop on Digital Identity Management*, 2006, pp. 55-62.
- [8] D. Davenport, "Anonymity on the Internet: why the price may be too high," *Commun ACM*, vol. 45, pp. 33-35, 2002.
- [9] C. Farkas, G. Ziegler, A. Meretei and A. Lörincz, "Anonymity and accountability in self-organizing electronic communities," in *WPES '02: Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society*, 2002, pp. 81-90.
- [10] D. Hardt, "ETech 2006 -- who is the dick on my site?" Sxip, [Feb 1, 2007]. Available: http://identity20.com/media/ETECH_2006/
- [11] M. B. Jones, "The identity metasystem: A user-centric, inclusive web authentication solution," [Jan 31, 2007]. Available: http://research.microsoft.com/~mbj/papers/InfoCard_W3C_Web_Authentication.pdf
- [12] A. Jøsang, J. Fabre, B. Hay, J. Dalziel and S. Pope, "Trust requirements in identity management," in *ACSW Frontiers '05: Proceedings of the 2005 Australasian Workshop on Grid Computing and e-Research*, 2005, pp. 99-108.
- [13] A. Juels, M. Winslett and G. Goto, in *"DIM '06: Proceedings of the second ACM workshop on Digital identity management,"* 2006.
- [14] B. R. Kim, K. C. Kim and Y. S. Kim, "Securing anonymity in P2P network," in *SOc-EUSAI '05: Proceedings of the 2005 Joint Conference on Smart Objects and Ambient Intelligence*, 2005, pp. 231-234.
- [15] "The Liberty Alliance," [Jan 31, 2007]. Available: <http://www.projectliberty.org/>
- [16] J. Miller, "Yadis specification 1.0," [Jan 31, 2006]. Available: <http://yadis.org/papers/yadis-v1.0.pdf>
- [17] R. L. Morgan, S. Cantor, S. Carmody, W. Hoehn and K. Klingenstein, "Federated security: The shibboleth approach," [Jan 31, 2007], Available: <http://www.educause.edu/apps/eq/eqm04/eqm0442.asp>
- [18] "OpenID," [Jan 31, 2007]. Available: <http://openid.net/specs.html>
- [19] D. Recordon and D. Reed, "OpenID 2.0: A platform for user-centric identity management," in *DIM '06: Proceedings of the Second ACM Workshop on Digital Identity Management*, 2006, pp. 11-16.
- [20] P. Sayer, "Seven pass latest liberty alliance conformance tests," [Feb 1, 2007]. Available: http://www.infoworld.com/article/07/01/16/HNpassconformancetests_1.html
- [21] T. Wright, "Security, privacy, and anonymity," *Crossroads*, vol. 11, pp. 5-5, 2004.