

A Single Sign-On Identity Management System Without a Trusted Third Party

Brian Richardson and Jim Greer

University of Saskatchewan, Department of Computer Science,
ARIES Laboratory, Saskatoon, Saskatchewan, Canada
{Brian.Richardson, Jim.Greer}@usask.ca

Abstract. Single sign-on identity management systems that rely on the use of a trusted third party, such as .NET Passport, face privacy and security risks when dealing with the management and storage of users' personal information. Presented in this paper is the design of a single sign-on system, which does not rely on the use of a third-party to manage users' personal information but at the same time allows users to present themselves to online businesses with more than one identity.

1 Introduction

Personalization of on-line content by on-line businesses can improve a user's experience and increase a business's chance of making a sale, but with stricter privacy legislation and Internet users' increasing concerns about privacy, businesses need to ensure they do not violate laws or frighten away potential customers. This paper describes the design of our Identity Management Architecture (IMA). The IMA system allows users to decide, on a per business basis what personal information is disclosed. It gives users greater control over their personal information held by on-line businesses, and does not rely on a trusted third-party for management of personal information.

In order to complete any commercial transaction on-line, people must provide personal information such as their name, address, phone number, email, credit card number, etc. On-line businesses often record more information than is actually needed to process a transaction. Some businesses monitor and record what types of products are bought or even the customer's browsing patterns. This is done to form a detailed profile that will allow the business to target a customer with future advertising of products more closely related to individual interests. As a result, businesses may be inadvertently in violation of privacy law and customers may be unaware of the extent to which their personal data is being stored or used. Individuals sometimes try to counter such actions by supplying false or misleading data in an attempt to conceal their identities. Thus, the following three factors formed the basis of this research:

1. Legislation: Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and how businesses can readily comply with this law [10].

2. Personal Concerns: The increasing concerns of Internet users about what information on-line businesses record about them.
3. Tool Support: The lack of an available privacy tool that allows for management of multiple identities.

Currently every popular personal information management system requires a third-party or a business to pass a user's personal information to another business. We believe that a personal information management system can be designed which does not rely on a third-party, and provides users with flexibility and control over the management of their personal information, while supporting business compliance with privacy legislation (such as PIPEDA). We also believe that privacy can be supported through the use of multiple identities by allowing a user to partition personal information into multiple pieces, each referred to as an identity. This would allow the user to choose on a per-business basis which identity to present. The use of multiple identities is a feature that is not yet offered by any commonly used personal information management system.

A Single Sign-On (SSO) system is one type of identity management system that allows a user to login to a system and gain access to numerous resources all with the use of a single username and password [14]. Systems like .NET Passport and Liberty Alliance allow for the use of a single username and password at multiple web sites, where the information for that one account can follow the user from site to site without the user having to re-enter information at each site visited, as long as that site is a participating member of that SSO service. These systems rely on some third party management of a user's personal information.

One common factor in most SSO systems is that they make the assumption that users always wish to present themselves online as the same identity with the same personal information. In fact people may not want all of their activities online to be linked to the same identity. Many people who use the internet will present themselves in with different identities when their purpose for using the internet changes. Each of these identities may contain some unique personal information with some overlap, and the owner of these identities would not want the activities taken while under each identity to be linked together. For example, if someone was considering finding a new job, he or she may not want the job hunt activities to be linked to a work identity for fear of his or her current employer finding out. It is for reasons like this that SSO systems need to realize the need for supporting multiple identities.

2 Background

Two SSO identity management systems have emerged in the consumer e-commerce arena. The Passport system (www.passport.net) was founded in 1999 by Microsoft. This system was designed to provide a single sign-in service that would allow Internet users to have one account for access to all Passport participating web sites [8]. The Passport system handles authentication of users by having the sign-in page on each participating web site authenticate the user by contacting the Passport system [8]. The Liberty Alliance Project (www.projectliberty.org) started in 2001 by Sun Microsystems to create an open standard, single sign-on authentication service [2].

The Liberty Alliance project has gained support from many well known organizations and now has more than 30 companies (e.g., Computer Associates, Hewlett Packard, Novell, etc.) involved in the development of the specification [2].

One of the main features of the Passport system is the single sign-in service. Although this is convenient, it does not allow for any sort of management of multiple identities. Passport does not allow the creation of multiple identities (i.e., more than one set of personal information) to be associated with a single account to allow a user to choose on a per business basis, what personal information a business receives. Although it is true that this could be accomplished by creating multiple Passport accounts, this defeats the purpose of a single sign-in service, since this approach would require a user to manage several Passport accounts, to remember multiple usernames and passwords, and to remember which account had been used at each business.

There is a misconception that Liberty Alliance is a similar service to .NET Passport. This is not the case. While .NET Passport is a single sign-on service implemented by Microsoft and used by online businesses, the Liberty Alliance Project is the development of a specification that can be implemented by businesses who wish to participate [11]. This specification allows businesses to form identity sharing relationships between each other and each implementation of the specification allows for this communication.

Liberty Alliance is based on the idea of allowing users to connect multiple sets of personal information, that exist across several on-line businesses, into one easy to manage identity. This allows for the convenience of a single sign-on service, as well as easier management of personal information across multiple businesses [1]. The Liberty Alliance architecture allows an Internet user to store his or her personal information with a trusted business. When the user needs to access a service provided by another business that is part of the same alliance of associated businesses, the user's chosen trusted business provides authentication of the user and forwards the user's identity information [1].

This system architecture is unique. Rather than relying on a trusted third party system, such as .NET Passport to provide a user's identity to each business the user accesses, it allows the user to have a business he or she trusts store and pass identity information from one business to another, which is part of the same group of associated businesses [1]. A group of associated businesses who have an agreement to share user identities and act as a single sign-on service is referred to as a Circle of Trust (COT). In a COT one business may act as the identity provider for a user and provide that identity to other businesses in the COT the user accesses [11]. One downside to this design is that identity management across multiple businesses is restricted to the set of businesses that have formed associations with each other. If a business is part of another group of associated businesses, identity information passing between these businesses is not available.

In early 2005, Microsoft announced that it was no longer going to pursue Passport as a solution for businesses to allow customers to manage their credit card and other personal information as they move from business to business online [6]. Companies such as eBay and Monster.com, two of the biggest non Microsoft companies to be using .NET Passport, who were initial supporters of the system, have dropped it in the last year. This, along with a lack of interest by many businesses and a failure of

internet users to openly accept Passport for storing their personal information, led to this decision by Microsoft.

There were concerns by companies about having Microsoft as the middle business between a company and its customers [6]. Users have been skeptical about storing their personal information in the Passport system. Anytime a user logs in to a Passport participating site, that site is immediately able to access all information in the user's Passport account [4]. Unfortunately for Microsoft, its systems often are the target of attacks by hackers, which has caused some embarrassment for Microsoft when security holes have been made public. A report by AT&T labs exposed several security flaws with Passport. One such flaw was that in order to compromise user accounts one only required a site that had a fake Passport login. This allowed usernames and passwords to be obtained providing access to all information in Passport about that user [4]. Microsoft also had to discontinue its use of the .NET Passport Wallet, which is a service that stored a user's credit card information, after it was discovered that all it would take to steal a person's Passport account and gain access to the Passport Wallet would be to get a user to open a Hotmail email [5]. Issues like this have raised continued concerns about security and privacy in the Passport system.

3 A Single Sign-On System Without the Third Party

In order to understand what makes our Identity Management Architecture (IMA) system different from existing SSO systems, it is important to understand the overall architecture of the system.

The IMA system is designed around two main components: the IMA Manager, which is the client application, and the IMA Web Service, which is the web service deployed by participating on-line businesses. Each business that wishes to participate in the IMA network must follow the standard defined for the IMA Web Service, must implement this service, and deploy it on its web site. Through this service, all interactions with the IMA Manager Client application are handled. Each user who wishes to benefit from the IMA network installs the IMA Manager application on his or her computer. This application ties into the user's web browser. Each person using the IMA Manager can create one or more identities, and then when visiting the web sites of participating businesses, choose which identity to associate with each business. For future visits, this identity will be used by default unless a different identity is selected by the user.

One of the key features of the IMA system, which is not offered by other personal information management tools, is the ability to create and manage multiple identities from within a single user account. The use of multiple identities does more than just restrict what information a business will see, but also allows people to interact with a business for more than one purpose. For example, if someone shops at an on-line computer parts store, sometimes for work purposes and other times for personal purposes, he or she may want to create a "Work" identity and a "Personal" identity. Creating separate identities allows someone to more easily manage these two separate relationships with a business. This may be beneficial to a business, especially one that personalizes web site content based on the interests of the user. If someone is using

his or her “Personal” identity, the business may use the browsed products and recently purchased products to make suggestions to the user about other products that may be of interest. If this same person visits the business’s web site at another time using the “Work” identity, the business will be better able to tailor content towards the interests associated with this identity.

One goal of the Identity Management Architecture is to avoid use of a trusted third party system and to not require businesses to communicate with each other for the purpose of providing a customer’s information. The IMA system has two main components:

1. IMA Manager (Client): An application that attaches to the user’s web browser and handles the management of all user identities and web browsing history.
2. IMA Web Service (Business): A web service that each participating business provides to allow users of the IMA Manager to send and receive identity information.

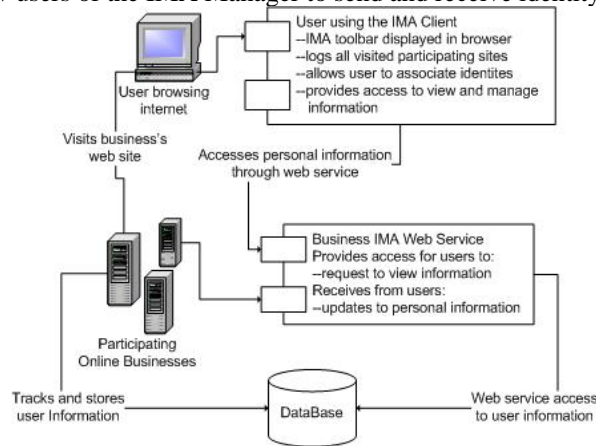


Fig. 1. The overall architecture of the IMA system: an IMA client application connects with a participating business using the IMA web service.

The IMA Manager allows a user to contact a business’s IMA Web Service to make a request to see what information the business currently has stored in the user’s profile. A user may correct or remove information. If the information to be changed is contained in an identity, a user may modify the identity information stored in the IMA Manager and the application will automatically forward updates to all businesses associated with this identity. The user may associate another identity with a business at any time; this will be used for future visits to that business.

As shown in Figure 1, the IMA Manager runs on the user’s local web browser. The Manager receives from the web browser the URL of each site the user visits while on-line. It then checks to see if the business is participating in IMA by attempting to contact the IMA web service that all participating sites are required to make available. If this business is not participating, then this is shown in the IMA Manager’s display. However, if the web service is available, this URL is stored and the service is contacted. The first communication with a business is the transmission of the user’s preferred on-line identity. From this point on, each time the user returns to this web site the user will be identified by this identity, allowing the business to asso-

ciate information, such as the products browsed, with this identity in order to determine the user's interests.

Only that information contained in a single identity is sent to a business. This is unlike Passport, which uses only one set of personal information for a user's account and provides it to each partner business. If a user wishes to have more than one identity, multiple Passport accounts must be created which defeats the purpose of a single sign-in service. The IMA system is designed to provide management of multiple identities on behalf of the user.

One additional key feature of the IMA system is that it provides users with the option to directly request what information a business has about them. The only information users have access to view and update with Passport is the personal information that was entered when the account was created. This does not provide users with any access to additional information a business has about them and it does not provide any benefit to businesses in terms of compliance with information disclosure requirements placed on businesses by privacy legislation.

With most personal information management systems (single sign-on services) it is necessary for either the user or service provider (or both) to establish additional relationships (i.e., with a third party system or another business) in order to be able to participate. The main goal of the IMA system is to provide the same types of services provided by traditional personal information management systems, but without requiring additional relationships to be established.

In order for users to participate in the .NET Passport system they must create an account with .NET Passport and provide all personal information they wish to be used in that account. This is the first new relationship that must be established outside of the traditional customer-business relationship. The second new relationship required is between .NET Passport and each business that wishes to participate (see Figure 2). These two new relationships require both users and businesses to be willing to participate in a personal information management system that involves a trusted third party.

The Liberty Alliance system allows users to select a business they trust to store their personal information. In order for this identity to be used at another business two conditions must be true: the business users are visiting must also be participating in the Liberty Alliance system and both businesses must have established an identity sharing relationship with each other (see Figure 2). If both are true, then users may use their accounts at other businesses and have their personal information transferred from the trusted business.

The IMA system relies on the existing customer-business relationship. If both the user and business are participating in the IMA system, personal information the user has in an account can be transferred to each business by the user (see Figure 2). The IMA system does not require a user or business to have to form additional relationships with either a third party system or another business.

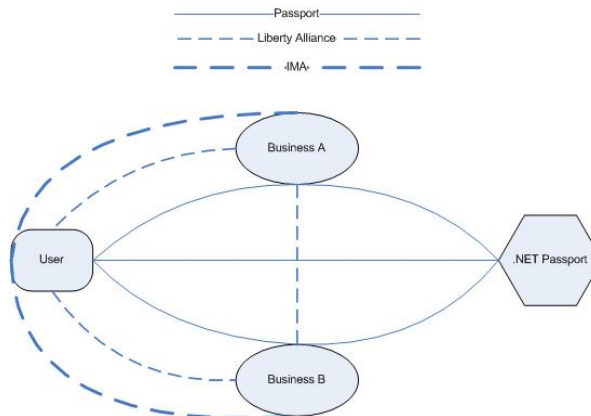


Fig. 2. Shown in this figure are the relationships that exist in .NET Passport, Liberty Alliance and the IMA network. As shown in the figure, Passport requires a user and business connection to a third party service, Liberty Alliance requires a business to business connection, while the IMA network requires neither relationship.

4 IMA System Implementation

In order to demonstrate the design of this system, a prototype implementation of IMA has been built. The implementation includes the client application as well as a sample implementation of the services associated with a typical participating business. Each component of the system has been written using the .NET framework [7]. Four components were implemented: IMA Toolbar, IMA Manager, IMA Web Service, and an example participating online business.

The IMA Toolbar is a .NET application that integrates into the user's web browser and provides the user with information on the participation of a web site being visited and the identity currently being used. This toolbar allows the IMA Manager to be automatically started when the user opens a web browser. This application is a class library that is registered as a toolbar with Internet Explorer and controls the IMA Manager. The IMA Toolbar created for this project was based on an example .NET Toolbar obtained from The Code Project [15].

The IMA Manager is a .NET application that runs in the background on the user's system. It is displayed as a taskbar icon, unless the user wishes to view the browsing history, or modify identities. This application is a standard windows application that displays a window when the taskbar icon is clicked.

The IMA Web Service is a .NET web service that allows the IMA Manager application to communicate with a participating business. Identity information is transferred to and from the IMA Web Service as an XML document. All other information recorded by the business that has been associated with the current identity can be retrieved in an XML document that the IMA Manager can display to the user who can make changes if necessary. How a business actually implements this system and how it ties into its database is the decision of the business. All that is required is that the

URL of the service and the methods offered match the ones required by the IMA Manager

To demonstrate the IMA system a small demo E-Commerce web site was built using ASP .NET. This site acted as a participating business providing the IMA Web Service that allowed the IMA Manager to be used to experiment with how the IMA system would work. This allowed for a better understanding of the IMA system design and also played a role in several design changes. The design of the IMA Manager and the IMA Web Service are described in detail in the following sections.

The IMA system allows users to set different identities, for example for personal, work, and private related activities. Having the ability to easily separate these identities allows web users to ensure that the information recorded about them at certain web sites is based on the identity they have assigned for that site. Users are able to select a single identity to be used for all web sites they visit, but they are able to switch to another identity when desired. The IMA Manager also allows users to view a list of recently visited business sites and modify defaults in order to have some alternate identity associated with any site at any time. This change results in the information for the alternate identity being immediately forwarded to the business. This alternate identity is then used for subsequent visits to this site.

When shopping at a number of different on-line businesses, it is convenient for customers to have each business keep some of their personal "account" information such as name and mailing address etc., and to connect to that account with a username/password. However, users are normally required to update account information manually at each business, when personal "account" information changes. The IMA Manager allows a user to update an identity and have those changes automatically forwarded to all businesses with which this identity has been associated.

If a business is participating in the IMA system, there may be no need for a first time visitor to the web site to have to fill out a long form to access a feature the business offers, as is often required for download of trial software. Instead, as the user accesses the site, he or she may choose to associate an identity with the business. Only after the IMA Manager receives confirmation from the user is the identity forwarded to the business by the IMA Manager.

4.1 Limitations

Personal information in the IMA system is always stored in two places; at the participating businesses the user has visited, and on the user's computer. Any responsible business will have security measures in place to protect stored personal information. However, the information stored on an individual's computer may be at risk of being compromised. In order to ensure no one other than the owner of the account has access to this information the account is stored in an encrypted, password-protected file. The user sets the username and password for an account when it is created. No one other than the owner of the account knows the password. Since there is no third party to store the account information or password, if the user forgets the password there is no way to retrieve it.

Even if an IMA participating business has excellent security measures in place to ensure each user's personal information is protected, there may still be increased security risks since this architecture promotes a more open exchange of personal information between users and businesses. If someone tried to make a request to a business for personal information while posing as another user, this could lead to the business disclosing a user's personal information to the wrong person. The way the IMA system attempts to reduce this risk is through the use of unique keys stored in each identity. When an identity is created, a unique key is generated and added to the identity. This unique key is used by businesses to authenticate an identity each time it is used. The key is never known explicitly by the user, but instead remains in the identity of the user account and is provided to businesses along with the other client-side information in the identity. In order for someone to pose as another user to retrieve identity information from a business, the impostor would have to know the key for that user's identity or be using the client computer of that user.

Another potential threat to the IMA system is that a disreputable business may not publicly state that it is participating yet may secretly deploy an IMA Web Service. Through this service the business may attempt to extract personal information from visitors to the business's web site if those users are using the IMA Manager. The result is that a business may try to collect personal information from users, yet not provide the required access for users to stored personal information. For the IMA Manager to release an identity to a business this action must be explicitly initiated by the user. First the user must be currently visiting the business's web site. Second the user must select an identity and attempt to associate it with the business. Third the user is asked by the IMA Manager to confirm the sending of the identity. The IMA Manager will never automatically release information to a business. If the user confirms that they want the identity sent to the business, then only at this time is this action taken by the IMA Manager. The IMA Manager makes every effort to prevent a business from receiving identity information without full knowledge of the user.

5 Related Work

There is currently extensive research work going on in the area of identity management by the Privacy and Identity Management for Europe (PRIME) [9] and The Future of Identity in the Information Society (FIDIS) [3] projects. Work by both of these projects has produced prototype identity management systems which each take a similar approach to handling of identities that allows users to switch identities (roles) based on which identity they wish to present to an organization. While both the PRIME [12] and FIDIS [13] projects are large in scope and are exploring in great depth many privacy and identity management issues, the IMA system really only attempts to address a small portion of the identity management problem.

The FIDIS project presents the prototype iManager which is the Identity Manager for Partial Identities [13]. Each partial identity contains a subset of the user's information that is applicable to the information needed for the user's current role, such as an identity that contains a credit card number and mailing address used when the user is shopping online. This approach is similar to how identities are handled in the IMA

system. Basically each identity in IMA, like partial identities, is identified and authenticated by a unique key that allows the user to be authenticated by an organization for all future visits using the same identity. This allows an organization to be able to track all repeat visits and associate information with that identity about the user, allowing the user to build up a relationship, regardless of whether or not the user has even provided his or her identifying personal information such as name, address, email, etc. A similar approach to the iManager's partial identities was followed in the design of the IMA system's multiple identity user account. The IMA system splits the user account up into identities which each contain a different subset of the user's personal information, identities such as anonymous, personal, work, school, etc. Each identity allows the user to only provide that set of information contained within the given identity, all other identities and information contained in the account are not disclosed to an organization.

The PRIME project presents the prototype IDM system [12]. The IDM system is a much more overall solution than the IMA system, however there are still some areas of IDM that the IMA system touches on. While the IDM system improves privacy by allowing the user to remain anonymous, even during a transaction, assuming there is a trusted third party that in the case of a problem (e.g., legal matter) the identity can be recovered, however in the IMA system no attempt to preserve anonymity like this is made. In the IMA system if a user decides to complete a transaction with a business, it is up to the user to decide whether or not he or she wishes to disclose an identity containing the required information, no anonymity is preserved in this type of transaction.

The primary goal of the IMA system was to build a single sign-on system that did not require third party storage or knowledge of user's information. As an additional feature the IMA system would also allow users to create and manage more than one identity from within a single user account where all identities could be accessed by a single username and password. These initial requirements were what the design of the IMA system had to achieve. Rather than comparing the design of the IMA system to the ongoing work in identity management taking place in PRIME and FIDIS, the IMA system was looked at more as an improvement upon existing single sign-on systems such as .NET Passport and Liberty Alliance. Both of these existing systems have well defined architectures which allow for a more detailed comparison to be made.

6 Future Work and Conclusions

Our next steps will be to build a larger, more complete implementation of the IMA system. The first issue that will need to be addressed is security. This will include determining the most secure way for a business to identify an IMA system user, and ensuring that only businesses authorized to receive the user's information have access to it. The second issue that will need to be decided is how to allow users access to their accounts from multiple locations. Since the IMA system does not rely on a third party system for account access and storage, the IMA system will require a different approach. There are several options available. One would be to store an encrypted

account file with a central service (whose trust level would be far reduced from that of the Passport approach). Such an approach allows for anonymous and secure storage of personal information in a "safety deposit box" that may be retrieved and used from various locations. A final decision on this matter has not been made.

The IMA system provides a design for a personal information management architecture that is offered as an alternative to .NET Passport and Liberty Alliance.

The main purposes of this research work are to demonstrate the benefits to a single sign-on system of increased access for users to their personal information and the allowing of users to maintain more than one identity. The main contribution of this project has been the design and development of an architecture for an identity management system that does not use a third-party or require businesses to transfer identity information from one business to another. It is hoped that this work will be the basis for more research into identity management systems (i.e., single sign-on systems) that provide users with more control over who can view or use their personal information, while allowing businesses to increase their compliance with privacy legislation, and improve the privacy of Internet users.

References

1. S. Cantor et al., "Liberty ID-FF Architecture Overview" 2003;
<http://www.projectliberty.org/specs/liberty-idff-arch-overview-v1.2.pdf>.
2. J. Evers, "EBay Cancels Its Passport" Jan. 2005;
<http://www.pcworld.com/news/article/0,aid,119137,00.asp>.
3. FIDIS, "Future of Identity in the Information Society"; <http://www.fidis.net/>.
4. S. Johnston, "Pondering Passport: Do You Trust Microsoft With Your Data?" Sept. 2001;
<http://www.pcworld.com/news/article/0,aid,63244,00.asp>.
5. B. McWilliams, "Stealing MS Passport's Wallet" Nov. 2001;
<http://www.wired.com/news/print/0,1294,48105,00.html>.
6. J. Menn, "Microsoft's Passport fails to travel far as Web strategy" Dec. 2004;
http://seattletimes.nwsource.com/html/business/technology/2002136272_passport31.html.
7. Microsoft, "Microsoft .NET Framework Developer Center";
<http://msdn.microsoft.com/netframework/>.
8. Microsoft, "Microsoft .NET Passport Privacy Statement" 2003;
<http://www.projectliberty.org/specs/liberty-idff-arch-overview-v1.2.pdf>.
9. PRIME Project, "Privacy and Identity Management for Europe"; <http://www.prime-project.eu.org/>.
10. Privacy Commissioner of Canada, "A Guide for Individuals" Nov. 2003;
http://www.privcom.gc.ca/information/02_05_d_08_e.asp.
11. P. Roberts, "Liberty Alliance Explains Its Sign-On Services" Feb. 2003;
<http://www.pcworld.com/news/article/0,aid,109277,00.asp>.
12. WP 14.1, "Framework V1" Mar. 2005; http://www.prime-project.eu.org/public/prime_products/deliverables/fmwk/pub_del_D14.1.a_ec_wp14.1_v1_final.pdf.
13. WP3, "Structured Overview on Prototypes and Concepts of Identity Management Systems" 2004; http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.pdf.

- 14.R. Yasin, "What is Identity Management?" Apr. 2002;
http://infosecuritymag.techtarget.com/2002/apr/cover_casestudy.shtml.
- 15.P. Zolnikov, "Extending Explorer with Band Objects using .NET and Windows Forms" Apr. 2002; <http://www.codeproject.com/csharp/dotnetbandobjects.asp?print=true>.