Abstract—this paper aims at studying two main solutions to digital identity management, Cardspace from Microsoft and Liberty from Liberty Alliance Project, and the problem of interoperability between them in a heterogeneous environment. It also proposes some recommendations for implementing the interoperability at some given levels.

Index Terms—Digital identity, Cardspace, Liberty, SAML, Web services, interoperability.

I. INTRODUCTION

INTERNET has become the most important means for communication in the information era. Thanks to the internet, users can do their online transaction without getting out of their houses such as shopping, buying train/airline ticket, etc. The fact is that many websites require the user to create an account with username and password, sometimes with other personal information. Before accessing to the site’s resources and ordering services, the user must to be authenticated with his account. With a boom in online services, internet users are having an ever increasing number of digital identities. These identities vary from site to site. From a practical point of view, the user tends to use the same username and password across different web sites to facilitate its online identities management. Apparently, from security point of view, this could be a major problem of privacy if user’s password was disclosed to non-trusted parties, we talk about identity thief.

Internet was not originally designed with the idea of digital identity and to resolve the problem of digital identity management, some solutions have been proposed and implemented amongst which we are interested in the two most widely used, they are Windows Cardspace (formerly known as InfoCard) and the Consortium Liberty Alliance.

In the first part of this paper, we’ll introduce these two solutions. This is followed by a comparison and the need for bridging the interaction between the two technologies. This need leads to the problem of interoperability between Microsoft CardSpace and Liberty Alliance at different levels. To illustrate this problem, we will then discuss about a general user’s case and existing solutions of interoperability. We also propose some recommendations for specific solutions within a given domain.

II. EXISTING IDENTITY MANAGEMENT SYSTEMS

A. Microsoft Windows Cardspace

After the failure of .NET Passport, Microsoft has recently introduced a new solution, called Windows Cardspace [5], which is designed on the law of identities and on the notion of identity meta-system. Cardspace is part of .NET framework 3.0 and integrated in Windows Vista as default (but also available in Windows XP and Windows Server 2003 Update). Windows Cardspace is a user-centric approach to digital identity management that provides users a friendly interface and a secure way to manage their online identities. Cardspace allows a user to issue his own card, called self-issued card or accepts cards issued by other identity providers, called managed card. These cards are also labeled as information cards. Information card does not carry any user’s information. Instead, it contains metadata in order to facilitate the retrieval of user’s personal information at identity provider side and reflects a reliable relationship between the user and the identity provider.

In the jargon of Cardspace, the service provider is called a relying party because it trusts on identity assertions of users released by identity providers. As depicted in the figure 1, in a typical scenario of Cardspace usage, there are 3 actors: internet users, relying parties and identity providers. As a user-centric solution, Cardspace technology involves a user agent installed at client side. This user agent is called card selector or occasionally identity selector and acts as a mediator between the relying party and the identity provider. In one side, it will receive and respond to relying party’s request. At the other side, it will require and get identity assertions from
the identity provider. This communication includes interaction with the user in order to ask for his consent to transmit his personal information.

When the user accesses to a relying party for ordering some products or services, the relying party requires user’s authentication. It will send to the identity selector a list of claims that it needs to know about user. The identity selector will search for all information cards available on the user’s PC and filter the ones satisfying relying party’s conditions. At this stage, it’s the user who has to choose a suitable card. The identity selector will contact the card’s identity provider to ask for a security token. In return, the identity provider will produce a security token and ships it to the identity selector that will present it to the relying party so that the user is identified and authenticated to access to relying party’s resources and/or services.

B. Project Liberty Alliance

Founded in 2001, Liberty Consortium [6] has assembled so far over 150 enterprises working on identity management solutions. And according to Liberty, there are over 400 millions Liberty-enabled entities and clients all around the world. Liberty Project solution is based on the notion of federated network identity and circle of trust in which service providers and identity providers establish a business relationship amongst them so that a principal (internet user in Liberty terminology) can perform business transactions in a secure and seamless environment. Liberty architecture is illustrated in figure 2 including three frameworks built on top of existing standards:

- ID-FF stands for Liberty Identity Federation Framework and as its name indicates, this framework provides the specifications for identity federation and simplified sign-on. It also supplies mechanisms for the termination of federation and for single log-out.
- ID-WSF stands for Identity-Web Services framework, provides specifications for identity-based web services. It defines a framework for creating, discovering and consuming identity services.
- ID-SIS is a collection of specifications that makes use of ID-FF and ID-WSF to enable networked identity services such as contacts, presence detection, wallet services, and geolocation services.

If a user wants to access service provider’s resources, the service provider will ask the user to choose an identity provider and the user is redirected to the selected identity provider. This identity provider will require to the user to authenticate himself with his account and to give him a security token. This security token will be forwarded to the service provider. The service provider will verify the token with the identity provider through a secured channel. As soon as the verification is terminated with a positive result, the user will be granted to access service provider’s resources. With the notion of identity federation, after being authenticated, the user can access to any service provider’s resource without being asked to log-in again within a circle of trust. If a service provider needs more personal information about the user, it can ask the identity provider to retrieve these attributes or it can retrieve these attributes within other service providers using Liberty specifications with the user’s permission.

C. Evaluation and Comparison

These two solutions are targeted to e-commerce and e-
government, accepted and supported by many big companies like France Télécom, Novell, Microsoft, IBM VeriSign, etc. they are built on existing standards such as XML/SOAP, WS-*., SAML, OASIS XACML, etc.

The most important difference between these two systems is that, Microsoft Cardspace doesn’t have any circle of trust [3]. And in comparison with Liberty Alliance, in Cardspace world relying party and identity provider must have compatible security policies to talk to each other. Microsoft solution stands on the user point of view and it’s an open architecture. By contrast, Liberty Alliance solution is built around a circle of trust to which the service providers and identity providers adhere by signing a business agreement. This helps identity providers to reduce their investments on the security infrastructure to identify the user. Liberty Alliance is a close architecture within a circle of trust.

Both Windows Cardspace and Liberty Alliance utilize the security token to identify the user at the service provider side but with Cardspace solution, the user has more control over his personal data to release as he is asked for his permission by the card selector running in his machine. Moreover, when the identity selector is triggered, it takes control over the machine so that it avoids some kinds of attack such as key logger, phishing.

Regarding privacy, in the second phase of Liberty Alliance, we see that it must have the user’s permission in order to share user’s attributes and with Liberty Advanced Client, identity provider cannot trace user’s activities and user keeps its attributes locally on his device. In Cardspace world, one drawback in privacy is that, if identity provider and service provider are under control of the same organization, the risk of being traced might persist.

III. INTEROPERABILITY OF IDENTITY SYSTEMS IN A HETEROGENEOUS ENVIRONMENT

In this section, we will talk about the problem of interoperability between Cardspace and Liberty Alliance through a typical case study and some existing solutions. We also propose some recommendations for a solution at a given level of interoperability.

A. Typical user case

In this user case, we will describe how a user can apply to a course offered by a remote university. In this scenario, we have 4 circles of trust with trust agreement signed amongst them. The circles of trust such as Electricity operator, Education support Liberty Alliance specifications while the circles of trust like City hall and banking supports Cardspace technology, as illustrated in figure 4. His high school and his targeted university belong to the same education circle of trust.

Now, he wants to apply to a Bachelor of Science (B.S) course by using university’s online application services. To complete his application, the university requires him to authenticate, provide his personal information, his high school record, his address certified by a trusted party and his credit card to perform the application’s fee payment. In the following, we will describe the online application service procedure step by step.

1. Firstly, the user accesses to the university website and selects the service of B.S. application. The site asks him to register and sign in. However it also proposes the user to sign in with other accounts in the education circle of trust. He chooses to log in with his high school account and begin his application procedure. The university web site asks him to fill in the personal information form manually or recommends him to allow it to collect this information from other partners’ website, and in this case, it’s done from the city hall website. He clicks on the button OK for this recommendation. After clicking, he is redirected to the city hall website. Normally, he has to present his Cardspace citizenship card to be authenticated. However, thanks to the federation of identity, he is seen as authenticated. The site asks him for his consent to send the sharable information to third party partner website, in this case university website. He accepts to share his personal information by clicking on the OK button. He will return to the university website to continue his application.

![Fig. 4. Typical user case](image-url)

2. Secondly, the website asks him to send his high school record by mail or send his certified electronic version of his high school record with a list of high schools. He selects his high school and then the following is transparent to him, just like the previous step.

3. Thirdly, university application services need his address certified by a third party so that the result mail will arrive at the correct destination. At this step, he chooses to use his electricity operator as the third party and the following is similar to the previous steps.

4. The last step, the user has to pay an application fee and the university offers him to pay by credit card. The university website proposes him to use a Cardspace credit card to perform the payment. He accepts this proposition and chooses a card to send. After this payment, the online application process is terminated.
This case study is elaborated in figure 4 with the relationship between different circles of trust. This is an imagined case because in reality, the user may have to do some other steps. This depends on university’s application policy.

This scenario shows two different levels of interoperability:

- How city hall, electricity operator and his high school can detect that he has already been authenticated. We are talking about the interoperability at the level of simplified sign-on (SSO) of intra-circle and of inter-circle of trust.
- How a Cardspace-powered service can gather user’s attributes in Liberty-enabled circle of trust or vice versa. We are talking about the interoperability at the level of attribute sharing.

B. Existing solutions

Until now, many efforts have been focused on describing and comparing distinct identity management systems such as in Higgins [7], Concordia projects [8] but few works aim to search solutions to the problem of interoperability between different identity management systems. Before addressing some issues to resolve the interoperability problem, we will describe principally two simplified sign-on solutions.

**Higgins Project**

Higgins [7] is an open source code internet identity framework, which was first introduced in 2006, is supported by IBM and Novell. Higgins project has performed some demonstrations at RSA Conference in April 2008 in San Francisco. Higgins defines a number of programming interfaces that developers can use to link their software to Higgins identity management functions. Higgins plans to release a middleware layer designed to supply identity services over data sources such as directory or database. The objective is to create a unique identity from all other identities of different domains. Higgins also intends to bring forth a security token service based on WS-Trust. Beyond these software components, the project is also developing a multi-platform client interface component called I-card being capable of interoperated with data of Cardspace. However, targeted applications of Higgins are essentially web applications and SOA programs.

**Integration Architecture at client-side**

Waleed A. Alrodhan and al. 2008 in [4] propose a solution that is based on the similarity between Liberty-Enabled Client profile and Cardspace data flow. They suggest to implement a software component within user’s machine that is able to talk to Liberty and Cardspace component and that is able to translate messages from Liberty language to Cardspace language or vice versa. The proposed solution is not easy to implement since it assumes that the web browser has to understand the data flows of CardSpace as well as those of Liberty Alliance.

C. Recommendations

The very first step to the solution of interoperability is mastering the differences and the similarities between technologies. At the level of authentication inter-circle of trust, To enable the passage from circle of trust A to B without re-authenticating, proposed solution must convert the security token from one perimeter to the other while conserving the information contained in the original token so that actors in the circle of trust B could understand the token presented by the newcomer. In the other words, the translation must not introduce the loss of information. This is not an easy task because the two technologies make use of different specifications and there’s also conflict between them. To some extent, the notion circle of trust somehow ambiguous. It requires some fundamental conditions to implement and in some circumstances, it could surprise users. Another possible solution is the mixed one. We do not pose the problem of SSO inter-technology. Instead, we try to associate and maintain the different sessions of users within different contexts and allow user to choose and change his aggregated identifier to represent him at visited sites. This approach seems to be potential because the characteristics of the two technologies remain intact and construct a bridge between them. However, it appears that a lot of work must be done not only at client side but also at server side.

IV. CONCLUSION

The interoperability is an ongoing problem and interesting research topic. The industry commences collaborating to search for solutions to this problem. Many projects has been founded and sponsored by industry giants such as Concordia, Higgins Bandit, OSIS, FC2, etc.

Solving this problem facilitate the deployment of unified identity solution across network and bring benefits to the internet user.

REFERENCES