# Windows CardSpace

Md. Faruk Hossain Mazumder, Mohammad Amdad Ullah Chowdhury
*Linköpings universitet, Sweden*
*Email: {farma067, mohch513}@student.liu.se*

## Abstract

*This report discusses about a critical security issue that is encountered by the modern internet user and the technology windows card space that is to be used to provide more secured way of maintaining user identity.*

*After analyzing the several aspects of this system we would like to compare the different type of Identity Management System with this system based upon some of the features they are focusing to the user like confidentiality, security and performance.*

## 1. Introduction

Today the use of internet has increased tremendously. Now user can do lot of online transactions (like buying ticket, order laptop, banking transactions). But these features also bring risks on security perspective like anyone might read the transaction; unauthorized user can modify the transaction while transaction is proceeding. Using username and password for authentication to access the web services is treated as one of the major problem from the security point of view. Because a password could be forgotten, it could be disclosed to unauthorized party when it is reused, it could be hacked by exhaustive search (searching with all possible combination) and above all it's management is not that much easy.

The Windows CardSpace is an approach to provide users more security and controlling power when disclosing their sensitive information to the other party in the online transactions.

Windows CardSpace is one type "of client software that enables users to provide their digital identity to online services in a simple, secure and trusted way" [1]. It is designed to manage users' digital identity in a very much secured way.

Three parties are involved in the total digital identity management process. These are the identity provider, relying parties and the users [1].

Identity providers are responsible to provide digital identity to the user. It stores all the related information of the user and provides this information to the relying party whenever the relying party asks for it. But before providing the information it again takes permission from user whether this information should be disclosed to the relying party or not.

Relying party is actually provider of service(s). To provide services to user; Relying party also need to identify the user and also sometimes need sensitive information of user (to complete the transaction). Because relying party don't know who is taking service from him. That's why relying party ask user to provide identification of him. Then using that identification relying party ask the identity provider to verify the user's information and to ask some other related information (which relying party need to provide this service) of user from the identity provider.

The most crucial point of identity management system is that, the user is always in a driving seat. That means it is only the user who has to select the correct digital identity and also has the control to select which kind of information he wants to disclose to the relying party [2].

The interaction among the parties to manage the digital identity is explored in the upcoming discussion of this article.

## 2. Background

"A digital identity is a set of characteristics (or "claims") by which a person or thing is recognizable or distinguished in the digital realm. Digital identity allows us to address an individual or thing without confusing it for someone/something else." [3]. Digital identity is also known as network identity.

### 2.1 Security Token


**Figure 1[5]: Security Token**

Security token is the key feature of all type of digital identity. It contains information of a digital identity in the form of byte stream. This byte stream represents claims. As a claim a simple token may consists of username only, where at the same time, a complex token may consists of credit card number, first name, last name, and home address. All the part of the claim is digitally signed by

using a private key to make sure that the claim is represented by the user who is authenticate of it.

## 2.2 Identity Metasystem

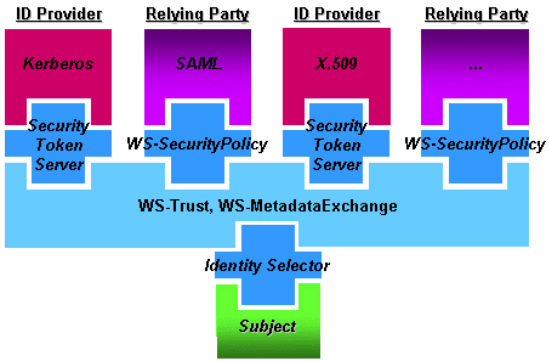


**Figure 2[6]: Identity Metasystem architecture**

Identity metasystem uses different technologies to communicate between the participants which are shown in the figure above. It includes the followings:

- Kerberos protocol, which provides secret key cryptography.
- X.509, which provides public key certificates for authentication purpose.
- SAML (security assertion mark up language) which enables user to log in different recognized websites.

The tasks perform by the identity providers, relying parties and the subjects/users are discussed below.

- **Relying parties**
  It specifies the required information through WS-Security Policy.
- **Identity Provider**
  "The Security Token Server implements the WS-Trust protocol and provide support for claims transformation" [6]. These claims contain the information specified by the relying party.
- **Subject**
  It maintains the interaction between the relying party and the identity provider. After receiving a claim from the identity provider it sends that claim to the relying party using identity selector.

# 3. Windows Card Space

The user interface of windows cardspace is provided with several cards as shown in the screen below. Whenever user needs any service from the relying party suppose any web server then the user needs to provide his/her digital identity for authentication.

The tasks required for this authentication process is discussed below.

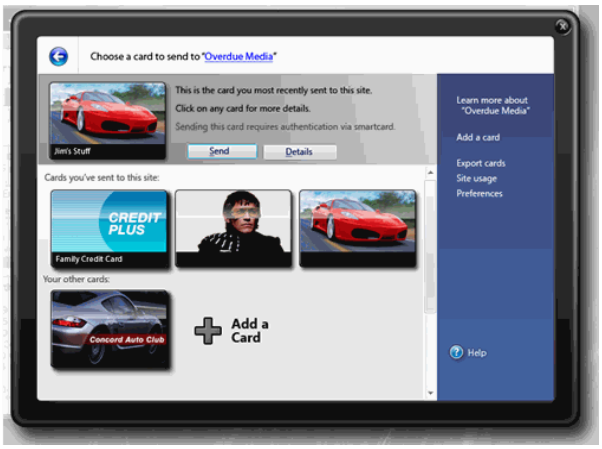


**Figure 3[5]: CardSpace identity selection screen**

Each digital identity is represented by a card. User can choose a card to represent his/her digital identity to a relying party. "Each card also contains information about a particular digital identity" [5]. The information indicates which identity provider to communicate to achieve a token "for this identity" and the type of token this identity provider can provide and the claims this token consists of [5].

By choosing a specific card, the user mainly asking for a particular token with particular claims "created by a specific identity provider" [5]. After getting the token user sends that required information to the service provider. User is not aware of the technical complexity of the entire process to manage the digital identity.

## 3.1 Windows Card Space Architecture

The backbone of the windows cardspace is the identity metasystem. In the windows cardspace identity provider might be user or any other external service. When identity provider is user then card is created by the user. But it has fixed set of claim not all features. Here data for the card is save into the user side. But it use security token using signing on the token. When identity provider is not user then both participants use SSL certificate to communicate between them. One example of this kind of identity provider is bank. Here identity provider issue managed card to user to identify the user.

Relying party could be two types. One could be when relying party is use web service. This type of relying party use standard web service protocol i.e. ws-*. When relying party use website then ws-* is not required. Here token is passing through the https using the post method.

To manage the digital identity three parties interacts as below

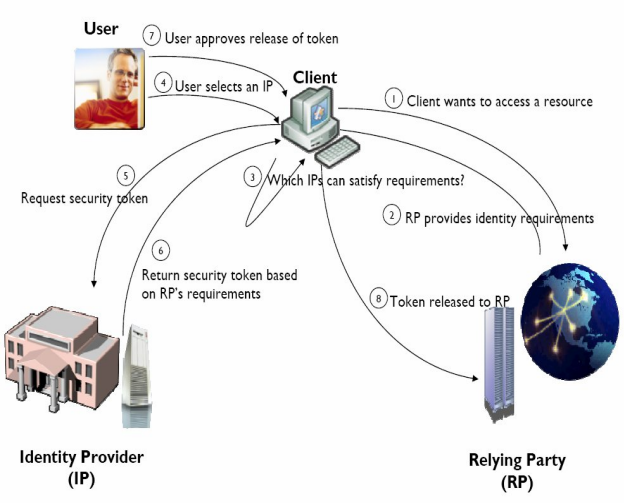


**Figure 4[4]: Workflow of Windows CardSpace**

- At first the client request service from the relying party.
- Relying party asks for identity to the user.
- Then the user chooses an identity of him to identify himself provider depending on the requirements of the relying party.
- Relying party asks for security token to the identity provider.
- The identity provider replies with security token depending on the requirements of the relying party. But before sending the token to the relying party it ask the user what should it disclose the token to the relying party?
- After the approval from the user identity provider sent the token to the relying party and then the user gets the required service.

### 3.2 Identity Provider and Security Measures

So far as we discussed, the parties that provides identity to the user is called the identity provider. Suppose, government may provide identities to its citizen, businesses may provide identities to customers [6]. Besides these, in windows card space architecture, users can also provide their own identity.

In both cases (self issued or other) identity provider creates SAML token in its machine (in case of self issued identity provider, token is generated in user's machine). This token contains user's information.

Furthermore, identity provider creates public and private key and uses the private key to sign the token. For security reason, this token consists of time stamp and other related information which ensure that no one else can use the token except the owner. And because of the timestamp, reuse of this token is also impossible. This token is then sent to the relying party "together with its associated public key" [5]. This public key is then used by the relying party "to validate the security token's digital signature, thus ensuring that the token is being presented by its rightful owner" [5].

It may seems, that the relying parties may cooperate together to observe "user's activities by comparing that user's public key" [5]. To prevent this phenomenon identity providers create separate "key pairs" for each relying parties [5]. This technique also prevents phishing sites to achieve user's identity.

If any relying party asks the permission to access the attribute of the user to the service provider then service provider cannot give information directly. To communicate between the service provider and the relying party both have to agree to the security policy and the stand of security technology what they will use during their data transformation like SSL.

## 4. Microsoft Passport

Microsoft Passport is another technology to authenticate user. In this technology user needs to create credentials (username, password) in the passport service. These credentials would be used to authenticate user to any web service that is in the Microsoft Passport Network.

User can fully rely on Passport Network because passport never observes users activity in the web. Suppose, which web pages user visiting or from where user making purchase. Passport Network only collects email address as user name and a password during the creation of an account to use these credentials to authenticate users to the web services. Even if a user doesn't want to use a real email address, user may choose one ending with @passport.com.

Passport maintains the authentication procedure using cookies. Whenever user wants to visit a website on the passport network, passport saves users identity and the time of log on, in a cookie which is stored in the encrypted form in users' machine.

Therefore, this cookie permits user to move several pages without logging in each time user visits a new page. When users sign out from the passport network, the cookies are deleted from users' machine.

## 5. Liberty Alliance

Another type of identity management system is liberty alliance powered by Liberty Federation. In the case of liberty alliance the identity is managed as a circle of trust where service providers don't need to invest money to create security infrastructure to identify a user. Security infrastructure is proving by the identity provider. There is a circle of service providers who is relying upon the identity provider. According to Liberty Federation's current figure more than 150 big companies and organizations has adopted with liberty alliance system [7].

## 5.1 Liberty Alliance Architecture

To communicate between the relying party, the service provider and the user there are two kind of system is using; they are identity federation and single sign on technique. In the identity federation, while logging to the identity provider if user select to federate with its other company in the same circle of trust then in the later while user want to log in to the other company in the same circle of trust then user information will be shared between them. So when user would log in there (different company in the same circle of trust) he will also get information from or related link from the main service provider though he logged in to the different authentication system. In the single sign on system if user log in to a main service provider then to visiting the other service provider site in the same circle of trust his login will be honored. So user doesn't need to log in to each of the service provider in the same circle of trust.

One concern about in those two login system is cookie. Normally cookie is a temporary variable used by the service to store information in the user computer. So after end of a transaction if cookie has not been taking care properly then it might be a vulnerability flaw. So cookie should handle properly to reduce the attack.

The basic interaction of user, relying party and service provider for both the identity federation system and single sign on system are in the following.

- User logs in to identity provider.
- Then the user access to service provider.
- Service provider sends some authentication request to identity provider.
- Service provider checks the authentication.
- User gets the service.

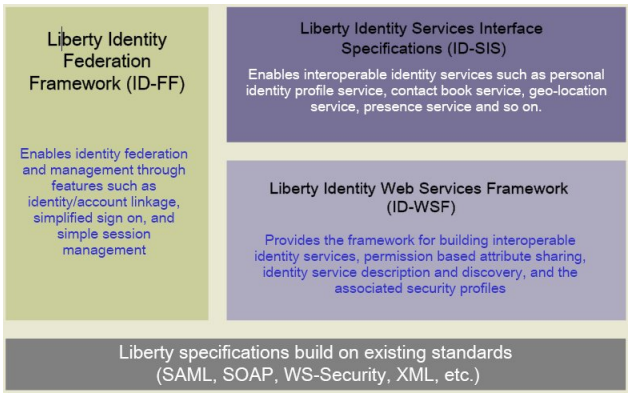


**Figure 5[7]: Liberty's Architecture**

In the liberty alliance architecture in figure 5 we can see that all the current liberty specification has been developed or going to be developed using the known web standards like SAML, SOAP, WS- Security ,XML etc. Liberty Identity Federation Framework is use to do the federation work and account management work. Liberty Identity Service Interface Specifications deal with the service like personal profile, geo location, contact book service etc. Liberty Identity Web Services Framework deal with identity services, attribute sharing depending upon user permission, policy establishment [7].

## 5.2 Privacy Policy in Liberty Alliance

To communicate the data properly Liberty Alliance has developed a generic architecture on the basis of "Usage Directives Container" which is called the Liberty Privacy Management Framework. Main goal of this specification is to before sending information between the relying party and the identify provider what will be the security policy standards between them. In this framework the participants agree with list of privacy policy they will use to communicate with each other [8].

Agreement between the participants is called the multilevel policy approach. Whenever the participants communicate with each other they insert the security policy header into the message. Whenever a relying party asks for some information of a user like name, address telephone number to web service provider containing the basic information of user from the identity provider then both the participants should come to one agreement how to collect those data. If the privacy policy of relying party is less or equal to the privacy policy of the identity provider then relying party will get those attributes from the web service provider at identity provider. Identity provider also inform them which way is optimum to transfer data like user interface base transformation or back end data transformation. The policy level may vary from strict to causal. In the privacy policies privacy strict is the most restrictive policy and privacy causal is the most liberal policy. There are five policies examples they are: privacy strict, privacy cautious, privacy moderate, privacy flexible, and privacy casual [8].

Every policy should contain what is the purpose the data, who will be the user of this data, retention policy of data etc. Privacy strict means that relying party can use the data for identity only, relying party must not share data with other but the replying party can keep the data as long as identify provider don't ask for reset the data. Privacy caution describe that party which is accessing this data will be able to use the data and his business partners can also use that data. Privacy moderate describe that other party can promote services depending upon this data but before promote the services they (service provider) should contact with the owner of data. Privacy flexible describes that data can also be shared with the others whose business is different from the seeker of data but seeker knows that which type of service they provide. Privacy causal describes that data can be shared with other party whose business is not relating to

the seeker of data and seeker also don't know which type of service they are providing to the user.

## 6. Evaluation and Comparison

If we compare windows cardspace with microsoft passport, we will find that windows cardspace is far more secured than microsoft passport.

In case of microsoft passport, when a user enters in to the passport network by signing in, microsoft passport stores authentication information in an encrypted cookie in user's machine. So, if user now reads an email from hotmail inbox which contains serious malicious code then there is a huge chance that users' identification is compromised with unauthorized party.

But in windows cardspace, identification token is provided by the identity provider towards the user. Now user decides whether to release this token to the service provider. And each time the user wants to access a new website different token is generated by the different identity provider according to the identification requirements of that website. So, here the users' identification information is much secured.

One of major difference between windows cardspace and liberty alliance is; windows cardspace doesn't has any circle of trust. So every service provider has to create infrastructure to identify the user. Meanwhile the basic of liberty alliance is circle of trust. Only one system is used to identify the user. So other service providers don't need to create infrastructure to identify the user. For that thing they are relying of the main identity provider which is also written as network identity providers. So it also cost effective.

Windows cardspace used single sign in technique where as liberty alliance use both single sign in as well as identity federation technique.

Both windows cardspace and liberty alliance use token to pass information to the relying party. But in windows cardspace user has more control to release the data to other as he has been informed by the window whether he want to release that data.

But one of the best features of windows cardspace is its easy to use. User doesn't need to put login information in the textbox. User just needs to select which card information he wants to send that's it. So it also decrease the possibility of phishing attack because may be some key tracker software is sensing the every key press. Here login also persist for long time up to the removal of the card. Another good feature of windows cardspace is control of data to release to the relying party. Every time user knows what information he is disclosing to whom. In that sense liberty alliance has less control over the data discloser to relying party and also in it user has to log in using username and password. So phishing attack might exist.

One drawback of windows cardspace is, till now it only supports windows operating system. So it also tough for service provider to implement the windows cardspace technology because may be all of their user will not be able to access it because of the operating system issue.

Sometimes user also doesn't look properly what information they are disclosing to whom. They just press the ok button. Windows cardspace is easy to develop and very little effort required configuring it.

## 7. Conclusions

In this report we explained architectures, operations and the technologies used in windows card space. We also discussed several other technologies like microsoft passport and liberty alliance and tried to show the comparison with windows cardspace over these technologies in terms of managing identities and security features.

Finally, we can say that windows cardspace is a tremendous approach of Microsoft to authenticate users to several web services with high security. It is not possible to deploy a technology which is totally secured but when the password system is proved very much vulnerable against the phishing and some other deliberate attacks, windows card space is proved to be much more secured against that type of attacks. To achieve the true benefit of windows cardspace users should also be aware whether a site is true site or a phishing site before releasing the security token to that site.

## References


[1] "Introduction to Windows CardSpace" accessed March 28,2007,from http://cardspace.netfx3.com/content/introduction.aspx

[2] Jones B. M. "A One-Page Introduction to Windows CardSpace", Microsoft Corporation, January 2007

[3] Frequently Asked Questions, accessed March 28,2007,from http://cardspace.netfx3.com/content/FAQ.aspx

[4] "Windows CardSpace and the Identity Metasystem" accessed March 28,2007, from http://cardspace.netfx3.com/files/folders/powerpoint_presentations/default.aspx

[5] Chappell D. "Windows Vista Technical Articles Introducing Windows CardSpace", April 2006

[6] Web Services Technical Articles Microsoft's Vision for an Identity Metasystem, Microsoft Corp. May 2005, http://www.identityblog.com/stories/2005/07/05/IdentityMetasystem.htm

[7] liberty alliance an overview, accessed April 25,2007,from www.projectliberty.org, www.projectliberty.org/liberty/content/download/752/5454/file/Liberty_Membership_Info_Sep04.pdf

[8] Liberty architecture framework for. supporting Privacy Preference Expression. Languages (PPELs),accessed April 27, 2007 from http://www.projectliberty.org/liberty/content/download/371/2670/file/Final_PPEL_White_Paper.pdf