GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN

Potentials and Areas of Application of the Windows CardSpace Technology

Seminar on Internet Technologies

by

Gunnar Nussbeck

Faculty of Mathematics and Computer Science
Institute of Computer Science

Date: September 30, 2008

Supervision:
Niklas Neumann

Contents

List of Tables

List of Figures

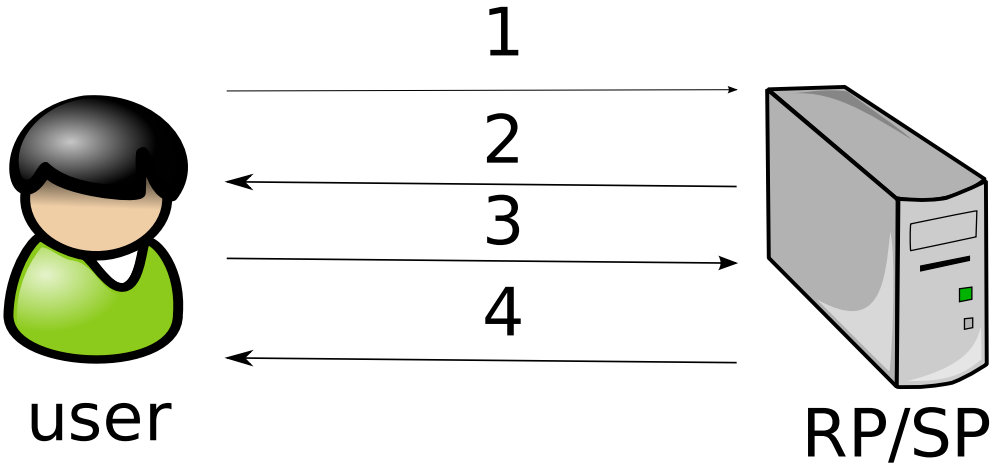
1 Introduction

Windows CardSpace is an id selector that uses Microsoft's ID-Metasystem as its back-end. It is designed to facilitate the usage of ID-cards for online communitation. It imitates the ease of use of id-cards that are used widespread in offline identity verification.

1.1 Motivation

The need for online id-management derives from various threats that are mostly security related. Cyber crimes like phishing, fraud, and ID-theft are increasing security related issues for e-commerce, that affect both users and service providers (SP).
Users want their private data protected against misuse, and are therefore reluctant to give their sensitive information to SP's they don't know or they don't trust completely.
On the other hand, SP's have to trust their online customers in respect to the data they provide. To protect themselves from fraud, most SP's need to check whether entered data like credit card information or addresses are correct or not for some costs.
In everyday offline business id-cards are issued by many parties. Some businesses have their own customer cards - like video stores or gyms, others rely on 3rd party id's like credit cards or student id. Some processes require official id's issued by governmental authorities - like drivers license or personal id-cards as an age verification device upon liquor purchase for example.
Today, users have to log on to every service they use while they surf the internet. They have to go through a verification process every single time they use a web service. This process can be seen in figure 1.1 on the following page: In the first step (1) the user request a service from a certain SP. The SP requests authentification information from the user in the next step (2). The user now sends his authentification information to the service provider (3). After successful validation of the authentication information, the SP provides the requested service (4).
This information flow is subject to several shortcomings. The users have to manage their different identities and their attributes. Without software assistance, this often leads to lost attributes or forgotten passwords that need to be recovered or reset. This process is sometimes expensive and time consuming. The SP's have to maintain their own framework for id-management. Additionally, the users can't estimate the trustworthiness of some providers. Cautious users won't give credit card information or other sensitive information like social security number or other personal attributes to unknown service providers. On the other hand, the SP has to trust the information like addresses or credit card information given by the user, or has to check them at high costs.

Figure 1.1: Typical information flow of an id verification process today.



1.2 ID Management Systems

Id-management systems implement standardized mechanisms for identification handling. Thus users don't have to use many different ways of logging in at different services, and they don't have to memorize lots of log-in data and passwords. This facilitates the everyday use of e-commerce, and makes it more secure due to elimination of insecure passwords or log-in credentials because auf password-fatigue. Password-fatigue is the phenomenon that occurs among many users. They are tired of memorizing unique passwords for all the online services they have accounts for. So users are likely induced to use the same password over and over, which impairs the password's security.
Id-management systems allow both users and SP's to securely share id-information from one single application. The user has to verify his id to the management system only once per session and therefore does not need to re-verify with different credentials over and over when he is checking his emails, shopping at online-stores and writing in boards or booking travels or concert tickets while he is surfing the internet. The secure communication of id verification through the management system reduces the risks of id-theft or fraud. Furthermore id-management systems open the opportunity of deploying single-sign-on for users in groups of web-services that trust each other. But the most important point is, that users become discerning about what information they give to whom. The benefit for service providers is, that they can outsource costly id-management and can use trusted third party identity providers to successfully prove their users' id's.

2 Windows CardSpace

In this chapter, I will give a high level overview of what Windows CardSpace does, and how it can be used to remedy the mentioned pitfalls of day-to-day id-management.

2.1 Mode of Operation

The design of CardSpace was driven by the following "laws" for id-management[1]:

1. **User Control and Consent:** The user should be in control of his/her information. He/she must be able to decide which bits of information to reveal.

2. **Minimal Disclosure:** No system that asks you for personal information is 100% secure. Hence I give only the information that is essential.

3. **Justifiable Parties:** When applying for social services, it makes sense to present a government-issued id-card. But when I gamble online, I'm going to use a different identity.

4. **Directed Identity:** I value my privacy. I don't broadcast it for everyone to see.

5. **Pluralism of Operators and Technologies:** No single identity system is going to suffice in all contexts.

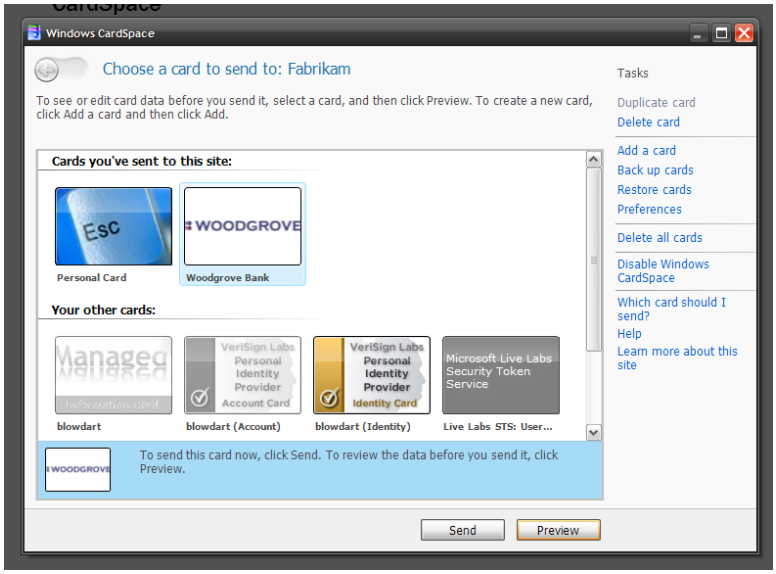
6. **Human Integration:** The end user must be considered the endpoint of the authentication protocol.

7. **Consistent Experience:** A stable identity system presents an easy-to-understand abstraction to the user that is considered no matter what underlying technology or identity provider is involved.

Figure 2.1 on the next page shows the CardSelector GUI of CardSpace. A web service (in this case Fabrikam) demands an id card. The selector now displays all available InfoCards and assists the user in selecting an appropriate InfoCard by showing which card meets the requirements, and if applicable, which InfoCard has been presented to the web service in earlier occasions. It also provides tasks which are necessary for InfoCard management like adding, duplicating, and deleting cards. CardSpace is shipped with the .NET Framework 3.0. It is installed on Windows Vista systems by default. It incorporates two different ways of obtaining an InfoCard: The first is to self-issue a card. This can be useful for web services that do not require to know my actual id, but want to identify me by my virtual

[1] Microsoft MSDN http://msdn.microsoft.com/en-us/library/ms996456.aspx

Figure 2.1: CardSpace GUI: CardSpace Identity Selector



id. The second method is to import 3rd party ID cards from different identity providers. This includes id-providers who provide id-management for web services as a mere service provider, or incorporated id-providers of web services like online banking or corporate network security departments.
Figure 2.2 on the facing page depicts a use-case diagram of a typical identifying process using CardSpace. First the user needs to obtain an InfoCard. This process is not included in this diagram, as it is only necessary to obtain InfoCards once for every ID one wishes to use. The identifying process starts with the users' request of the service (1). The Identity Selector now requests the security policy from the Relying Party (RP) (i.e. the service provider) (2). After receiving the policy (3), the Identity Selector takes over the control from the user and determines all appropriate InfoCards, that meet the policies criteria (4). The Identity Selector now presents all possible InfoCards to the user (5). The user chooses the card he wants to use, and thereby selects the identity provider to use (6). The Identity Selector now requests the security policy for the selected InfoCard from the id-provider (7). After receiving the policy (8), the Identity Selector requests the security token with the claims required by the RP (9). The RP returns the requested token (10), and the Identity Selector presents it to the RP, requesting access to the service (11). The RP now grants access to the service (12), and the user gains access to the identity aware service he requested in step 1 (13).
One can see that the process control is mainly in users' hands. Only for a short time, while determining appropriate InfoCards, the Identity Selector takes over the control.
In this process, the term claim is used to determine any information token that is to be proven. Table 2.1 on page 8 shows such claims that are commonly

Figure 2.2: CardSpace: Use case diagram of a typical id process, Source: Microsoft MSDN msdn.microsoft.com/

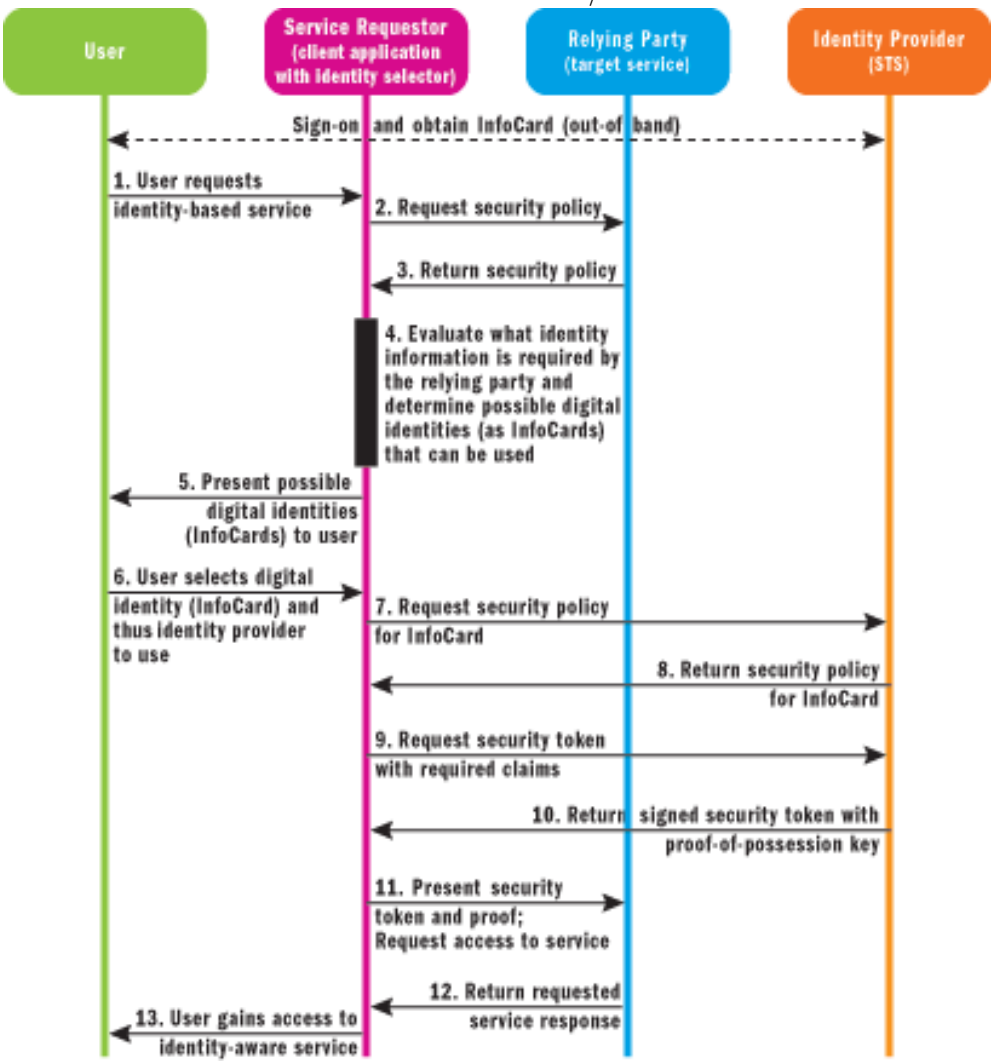


Table 2.1: Claims typically used in InfoCards

Claim	**URI Suffix**
First name	givenname
Last name	surname
E-mail address	emailaddress
Street address	streetaddress
Locality name or city	locality
State or province	stateorprovince
Postal code	postalcode
Country	country
Primary/home telephone number	homephone
Secondary/work telephone number	otherphone
Mobile telephone number	mobilephone
Date of birth	dateofbirth
Gender	gender
Private personal identifier	privatepersonalidentifier

used in InfoCards. The list is not limited. Some claims are optional, and 3rd party providers may add additional claims. The claims do not contain any highly sensitive information like credit card number, social security number or so. But even the combination of name, date of birth and full address are sensitive, because they clearly identify a person.

2.2 Capabilities

This section deals with the capabilities of CardSpace. It deals with what services are eligible to use CardSpace, and what technical requirements are to be met. Windows CardSpace is built on top of the web services protocol stack (ws-*) which inculdes WS-Security, WS-Trust, WS-MetadataExchange and WS-SecurityPolicy. To implement CardSpace capability into a website, the developer simply needs to declare a HTML ⟨object⟩ tag, that specifies the claims the website is demanding from the user

```
1 <object id="informationCards" name="informationCards"
    type="application/x-informationCard" >
2 <param name="issuer" value="http://schemas.xmlsoap.org/ws
    /2005/05/identity/issuer/self"/>
3 <param name="tokenType" value="urn:oasis:names:tc:SAML
    :1.0:assertion"/>
4 <param name="requiredClaims" value="http://schemas.
    xmlsoap.org/ws/2005/05/identity/claims/
    privatepersonalidentifier http://schemas.xmlsoap.org/
    ws/2005/05/identity/claims/emailaddress"/>
```

```
<param name="optionalClaims" value="http://schemas.
   xmlsoap.org/ws/2005/05/identity/claims/dateofbirth"/>
</object>
```

and implement code to decrypt the returned token and extract the claim values. This example uses Microsoft's TokenProcessor assuming that the encrypted token is stored in the hiddenXmlToken variable.

```
string token = Request.Form["hiddenXmlToken"] as string;
if (!String.IsNullOrEmpty(token)) {
  Token tokenProcessor = new Token(token);
  string ppid = tokenProcessor.Claims[ClaimTypes.PPID];
  string emailaddress = tokenProcessor.Claims[ClaimTypes.
     Email];
  string dateofbirth = tokenProcessor.Claims[ClaimTypes.
     DateOfBirth];
}
```

The web service has now access to the requested claims. For an improved user experience, InfoCards can be linked to the user's account in the user database of the SP. Both listing examples are taken from Microsoft's Developer Network pages. The whole ws-* set of protocols is part of Microsoft's Open Specification Promise. This grants that the specifications are and allways will be free to use for everyone.
More options information on how to use CardSpace can be found at the CardSpace API documentation page[2].
Not only does CardSpace replace the username / password login, it also can prove claims that do not identify a specific individual, but merely a membership to a group of users. For example that a user is of legal age to use certain services. Also claims like "I am student of university X" can be proven to grant access to institutional services, and more important to access 3rd party services or to prove eligibility to student discounts.
The id-metasystem CardSpace is build upon is token format agnostic, which means that CardSpace can be used with various services. It even can be used to log into OpenID providers, WindowsLive ID and such. This renders single sign on possible while surfing the web. The user signs on to an CardSpace aware IdP A, and henceforth every web service he requests during that session can authenticate the user if he also accepts IdP A.

[2]http://msdn.microsoft.com/en-us/library/aa702727.aspx

3 Discussion

Microsoft states, that CardSpace does not compete directly with other Internet ID architectures like OpenID and SAML, but they complement one another[3].
The benefits of CardSpace are, that it enables the user to deal with his personal data in a secure and easy to use manner. The average user is mostly not aware of security risks. CardSpace minimizes these risks by assisting the user to determine the security and trustworthiness of web services. CardSpace does not reveal more information than needed to 3rd parties, so the user keeps the control over his information. CardSpace is widespread because it is shipped as a standard feature with Windows Vista, but also selectors for other operation systems support the protocols used by CardSpace[4]. This
Shortcommings of the CardSpace architecture are, that accounts are not, or not easily transferable. One can export InfoCards, safe them to thumbdrives, and import them on other machines, but that is neither practicable, nor secure. Also, there is no possibility to use CardSpace from shared computers (e.g. in public libraries or internet cafes). As a remedy, a CardSpace Selector capable of reading encrypted thumb drives is announced, but not yet released. The single layer of authentication throughout a session renders session hijacking possible.[5]
Overall, CardSpace enables the user to manage his identity and private information. It can not be considered as one hundred percent secure, but it arouses the awareness of average user's to their data privacy without overburden them with complicated systems they won't use anyway.

[3] http://netmesh.info/jernst/Digital$_I$*dentity/three − standards.html*

[4] "Internet Scale Identity Systems - An Overview and Comparison", PingIdentity Whitepaper, Feb2007

[5] Waleed Alrodhan and Chris J. Mitchell: "Addressing privacy issues in CardSpace", Third International Symposium on Information Assurance and Security