E

Understanding Windows CardSpace

Identity and access controls play a fundamental role in building connected systems. They are required either implicitly or explicitly, in almost every interaction. If they are taken away, misused, or harmed, the consequences can be awful. However, it is only recently that most people have started taken care of their identity, its usage, and illegitimate use because of the popularity of the connected computer systems, such as Local Area Network (LAN), Wide Area Network (WAN), and the Internet. When the Internet was not prevalent, securing identity information was not a major issue.

Today; however, things have changed drastically. Irrespective of all the convenience, power, and potential, many people are actually reducing their usage of the Internet, particularly with respect to online purchasing. Statistics show that just as the usefulness of the Internet is increasing, the trust in it is decreasing. This is because of the various problems sprouting with online identity, such as phishing.

Therefore, it means that the solution is to find a logical way to use multiple digital identity systems, without security issues. This implies that a system of systems known as a metasystem is required, which focuses completely on identity. Microsoft has played a major role in defining this standard-based identity metasystem. It is also adding new capabilities to Windows to help make the identity metasystem a reality through Windows CardSpace, originally code-named InfoCard.

Windows is one of the most widely used operating system all over the world, and so, CardSpace plays an important role in making the identity metasystem real. However, this solution cannot be successful unless other organizations also implement it in their systems. Microsoft is actively encouraging the creation and use of software that can participate in the identity system of systems-a metasystem. The goal of Microsoft is to allow users on any machine, running any operating system, use digital identities easily, effectively, as well as securely as they today use their identities in the physical world.

In this chapter, you learn about digital identity. Next, you learn the use of security tokens for digital identities. In addition, you learn about the functioning of Windows CardSpace.

Understanding Digital Identity

Similar to identities in the real world, such as your driving license to prove that you are a valid driver, you are provided with digital identities. For example, if you have an e-mail account with `Gmail`, you will be identified by an e-mail address. You might also have digital identities with various commercial organizations, such as `Rediff` shopping or `eBay`, along with identities for social networking sites, such as `Orkut.com`. Each of these is typically identified by a username defined by you. Nowadays, at most workplaces, you have a digital identity assigned to you by your employer, which is identified by your network login. This identity is most likely maintained by some directory service, such as an Active Directory, and is typically useful only within the boundaries of your company's network.

There are several positive reasons to use different digital identities in different contexts. For example, an identity that you use with Rediff shopping might allow access to your credit card number, while one used with Orkut.com does not. The conventions for getting each identity are also different. Getting a digital identity at Rediff shopping is much easier as you just need to create a user account. However, getting a digital identity at your employer (organization you are working) is probably to some extent more difficult, as it requires the approval of the administrators running your company's network.

Using Security Tokens for Digital Identity

Digital identities available in the real world, though varied in nature, have one important thing in common. When they are transmitted on the network, they are represented by some kind of security token. A security token is a set of bytes that provides information about a digital identity. Figure E.1 shows the structure of a security token:

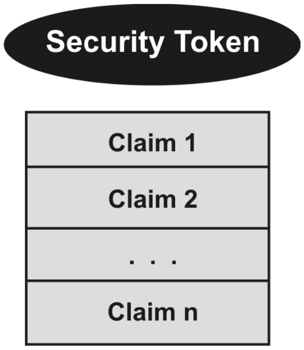


Figure E.1: Displaying a Security Token

A security token contains information of one or more claims, each of which contains some part of the total information conveyed about the identity. For example, a simple security token might include only a single claim containing a username, while a more complex one might include claims containing a user's first name, middle name, last name, and address. Security tokens for some digital identities might also include claims that contain sensitive information, such as your credit card number.

Most security tokens provide some information to prove that the claims belong to the user who is presenting them. One very practical approach of proving that the claims belong to the user presenting it, which is common these days, is to send a password along with the claims. You can make this approach more effective by digitally signing all or part of the claims by using a private key, and then providing the corresponding public key to the digital identity, possibly wrapped in a certificate. The security tokens that represent digital identities commonly provide some kind of proof that allows a receiver of the token to verify that this token really represents the intended individual or that the user has an association with that identity.

Conventionally, digital identities have been used primarily for authentication purpose. For example, your voter id includes your name, age, your picture, and other information, all asserted to be correct by the governmental organization of your country. Nowadays, the most common security token formats are userid and password credentials, X.509 certificates, SAML-Assertion and Kerberos tickets, because the information they carry is largely focused on authenticating an identity. A digital identity that expressed this information is useful for proving various other things. Similarly, each of your credit cards carries a card number, your name along with date of issue, and an expiry date. Just as these cards are useful in the physical world, it will also be useful to create a digital identity for each card that can be used to generate a security token carrying proper claims.

Even though security tokens have been traditionally focused on conveying just authentication information, it is important to understand that the idea of a digital identity is quite broader than this. By using Security Assertion Markup Language (SAML) or other approaches, it is possible to define security tokens that contain a large amount of any desired information. Digital identities have now become as broadly useful in the networked world.

Functioning of Windows CardSpace

CardSpace converts your personal or provider cards to special tokens and validates their authenticity on demand. Different card types use different tokens for these validations. Personal cards use Security Assertion Markup Language (SAML) 1.1 token types by default. However, provider card tokens are subject to organization's technology preferences. For example, a bank card, such as credit card or debit card, has a magnetic strip on the back of it. This strip stores account holders' claims in the bank system.

NOTE

CardSpace is already supported by a Java toolkit from Ping Identity

Windows CardSpace works on the concept of metaidentity, that is, it supports multiple identities. This support (of multiple identities) is much more scalable than a single identity system, such as passport. Therefore, you can utilize multiple identities on diverse platforms to validate identities using CardSpace.

To know whether you have CardSpace available on your system or not, perform the following steps:

1. Click Start→Control Panel. The `Windows CardSpace` icon in Windows 7 is displayed as shown in Figure E.2:

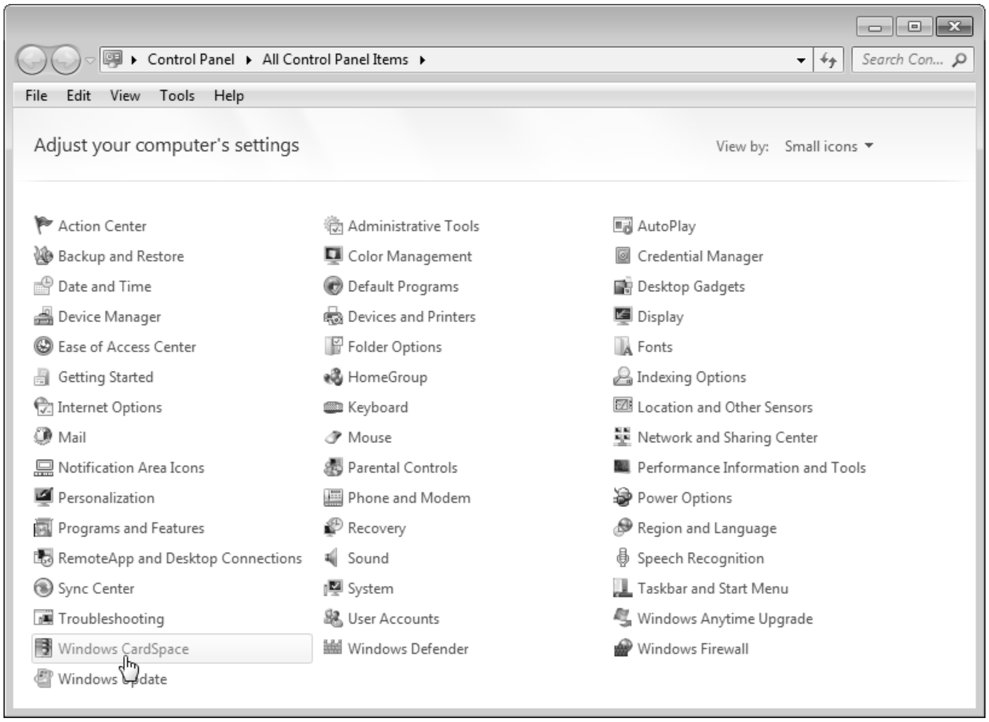
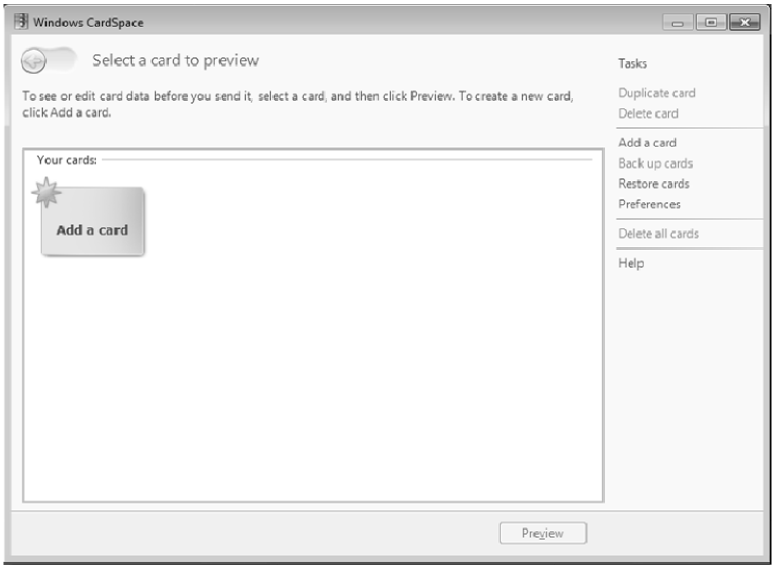


Figure E.2: Displaying Windows CardSpace in Control Panel

2. Double-click the Windows CardSpace icon. The Windows CardSpace screen opens that helps you create personal cards and provider cards, as shown in Figure E.3:

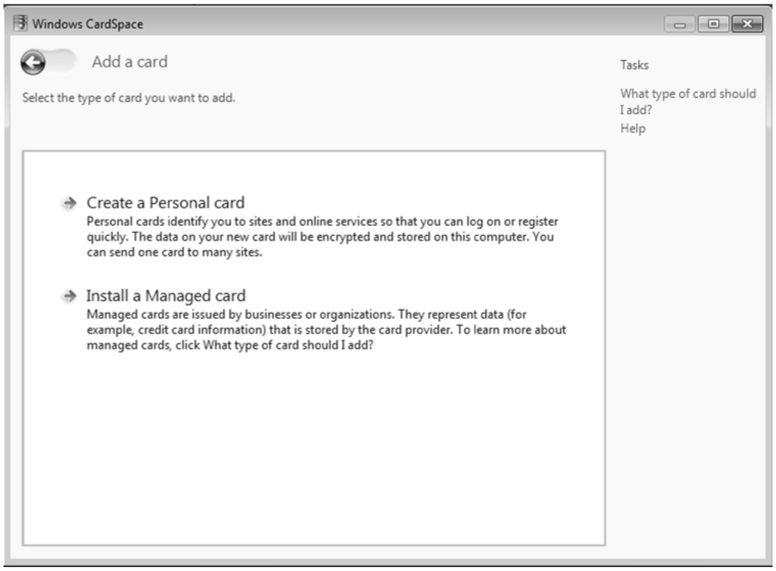


To see or edit card data before you send it, select a card, and then click Preview. To create a new card, click Add a card.

Figure E.3: Displaying the Windows CardSpace Screen

The Windows CardSpace screen acts as a container for all your identity needs.

3. Click the `Add a card` option to see the type of card options, as shown in Figure E.4:



Select the type of card you want to add.

Create a Personal card
Personal cards identify you to sites and online services so that you can log on or register quickly. The data on your new card will be encrypted and stored on this computer. You can send one card to many sites.

Install a Managed card
Managed cards are issued by businesses or organizations. They represent data (for example, credit card information) that is stored by the card provider. To learn more about managed cards, click What type of card should I add?

Figure E.4: Displaying the Type of Cards Options

Windows CardSpace provides the following two types of cards:

- **Personal card**—Refers to the card that is based on the self-issued identity providers
- **Managed card**—Refers to the card that is based on the identity providers provided by the vendors other than Microsoft

With this, we come to the end of this appendix wherein we have learned about digital identities and the working of security tokens.