Patterns for Supporting Information Cards at Web Sites: Personal Cards for Sign up and Signing In

---

Microsoft Corporation

Published: April 2007

Authors: Bill Barnes, Garrett Serack, and James Causey

Abstract

This document describes patterns for implementing Personal Information Card support on Web sites. Web site developers can use this document to create sites that take advantage of Information Cards to improve the ease of use and security of their user experience.

Contents

Supporting Information Cards on Web Sites

Users of Web sites today face a set of common problems. Determining the legitimacy of sites is often difficult. In addition, the traditional method for users to identify themselves to a Web site—password authentication—contains a number of flaws. Web site developers can address these issues by supporting Information Cards.

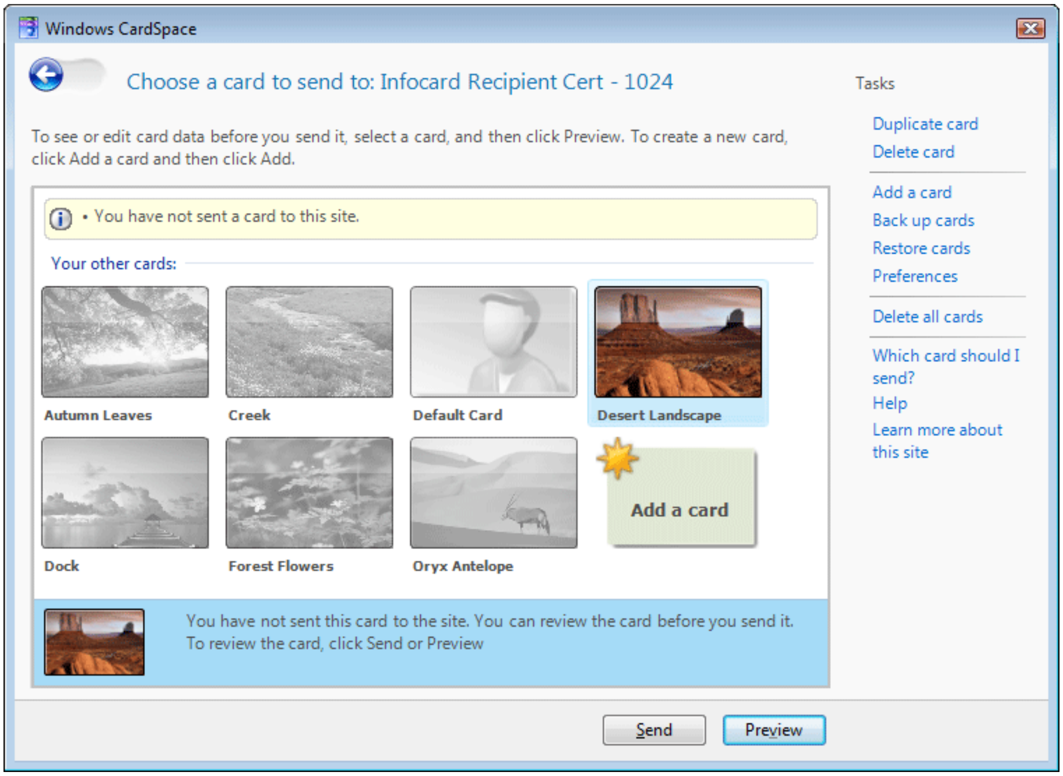
Information Cards provide a visual representation for digital identities that a user may have. The user can use Information Cards to select which digital identities to employ at different Web sites. Information Cards provide users with a simpler and safer experience that is very similar to the card experience that they have in the physical world. Web site developers can accept Information Cards to simplify user registration and sign-in.

After meeting a set of basic prerequisites, Web site developers can support account registration and sign-in using Information Cards without having to alter their session management procedures. Developers can also support the use of Information Cards along with traditional password authentication techniques. These distinct techniques can complement one another or provide alternative authentication options for users. In addition, developers can provide for recovery of lost Information Cards to regain account access.

Information Cards

Information Cards are virtual representations of a person's identity that are assured by a particular party. Information Cards are analogous to real-world identity cards such as passports, driver's licenses, credit cards, and business cards.

Information Cards are managed and issued on client computers by a piece of software called an Identity Selector. An Identity Selector is a security-hardened user interface (UI) that appears when a user attempts to authenticate to a Web site that requests an Information Card. The following figure shows Windows CardSpace™—the Microsoft implementation of an Identity Selector for Microsoft® Windows®—in response to a demand for credentials by a Web site.



Choose a card to send to: Infocard Recipient Cert - 1024

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 and then click Add.

• You have not sent a card to this site.

You have not sent this card to the site. You can review the card before you send it. To review the card, click Send or Preview

Each Information Card represents one or more claims about a user's identity. These claims can be as simple as a person's name, and they can also include a wider range of information. Web sites can consume these claims for the purposes of sign-in and registration, as well as for other purposes. For more information about identity claims, see "Claims" in Managing Information Cards with Windows CardSpace (http://go.microsoft.com/fwlink/?LinkId=87314).

Information Card interactions on the Web involve three participants:

- The user, who holds Information Cards that represent one or more claims
- Web sites, which accept the claims that the user presents through an Information Card
- Identity Providers, which issue digital identities that are represented by Information Cards

For example, a company may issue Information Cards for its employees or for customers. Individual users may also issue Information Cards for themselves.

A Personal Information Card is a card that is generated and assured by an individual, while a Managed Information Card is a card that is generated and assured by a third-party Identity Provider.

Note:

> This document focuses on Personal Information Cards. For more information about the types of Information Cards and their use, see Managing Information Cards with Windows CardSpace (http://go.microsoft.com/fwlink/?LinkId=87314).

Different cards may be accepted in different situations. An individual normally carries multiple types of identification. For instance, it is common to carry a driver's license, business cards, credit cards, and a library card all at once. Information Cards are designed for a similar experience, in which a user can maintain different cards of different types—each designed to be presented in one or more situations.

Advantages of Information Cards

Information Cards are more flexible than simple user names and passwords. Information Cards employ strong cryptography, which makes their use more secure than passwords. Information Cards can potentially present any type of identity claim that makes sense to all of the interacting parties and which users are willing to release. Potential scenarios may include the use of verified identity attributes, such as age or even payment information, which makes it possible for Information Cards to be used much like a physical credit card during an online transaction.

Note:

> This document does not cover advanced scenarios, such as age verification or online payment solutions.

Finally, Information Cards can be supported easily alongside a traditional password authentication system, which enables a smooth transition for users from passwords to Information Cards.

The Information Card model is built on open, interoperable communication standards that have been implemented on Windows and other platforms. This interoperability enables Web application developers to move Internet interactions beyond password authentication, regardless of their underlying platform or the platform of their clients.

Implementing Information Card Support

Support for Information Cards involves a number of common scenarios, including signing up to a Web site, signing in to the site, recovering an account if a user loses their Information Card, and detecting client support for Information Cards.

Preparing Your Site

To prepare your site to accept Information Cards, you must complete a few preparatory steps:

- You should be comfortable with Web application development using Hypertext Markup Language (HTML) and authentication of some kind, such as forms-based authentication.
- Acquire and install a Secure Sockets Layer (SSL) certificate. Information Cards rely on SSL encryption to help secure communications between the user and the Web site. Identity Selectors, such as Windows CardSpace, only invoke from a Secure Hypertext Transfer Protocol (HTTPS) page with a valid certificate.

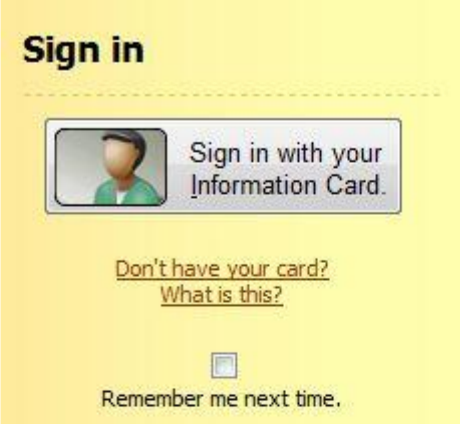
  Some certification authorities are issuing a new class of SSL certificate, known as an Extended Validation (EV) certificate. EV certificates are issued under more stringent identification guidelines. However, Identity Selectors are able to make stronger statements about the identity of a site that is associated with an EV certificate. We highly recommend EV certificates for sites that can meet their requirements.

  Note:

  Each SSL-secured Web site must have its own SSL certificate to invoke Identity Selectors.
- Configure time synchronization. Security tokens include time-stamped validity intervals to protect against man-in-the-middle attacks. Web developers can use protocols such as Network Time Protocol (NTP) to guarantee correct local time and validate those time stamps.
- Write and deploy a privacy policy Web page. Identity Selectors can download the privacy policy's pages directly from that URL and display them to the user as part of the card selection process.

Enabling Information Card Sign-Up

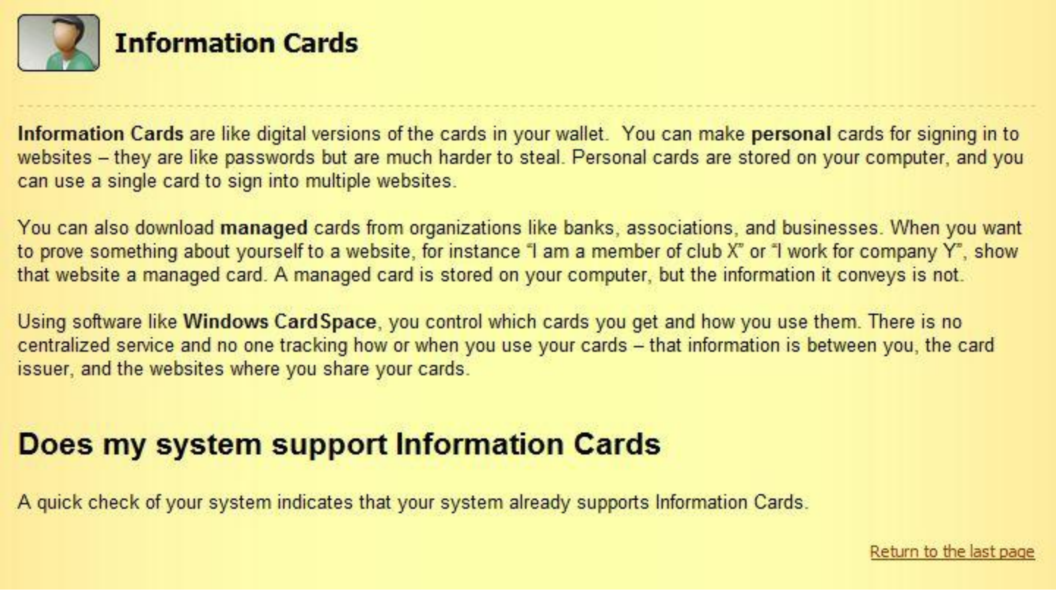
Users who visit an Information Card–enabled site experience a streamlined sign-up process. You can present your users with a familiar UI that encourages them to sign up with an Information Card, as shown in the following figure.



This UI displays a button for signing into the Web site. When a user clicks the button, the Identity Selector will be invoked and the user can select their card for signing in. If the user wants the site to remember them for next time, they can select the check box (“Remember me next time”). Note: a site can remember users using existing mechanisms, such as cookies. Using Information Cards does not change this.

This UI also includes two links. Users can use the first link ("Don't have your card?") to recover lost Information Cards. For more information about this scenario, see "Enabling Information Card Recovery."

The other link ("What is this?") helps users learn more about Information Cards, how they work, and whether the client platform supports them. The following figure shows the description that appears when a user clicks the "What is this?" link on a Windows computer running Internet Explorer 7.



Information Cards

Information Cards are like digital versions of the cards in your wallet. You can make **personal** cards for signing in to websites – they are like passwords but are much harder to steal. Personal cards are stored on your computer, and you can use a single card to sign into multiple websites.

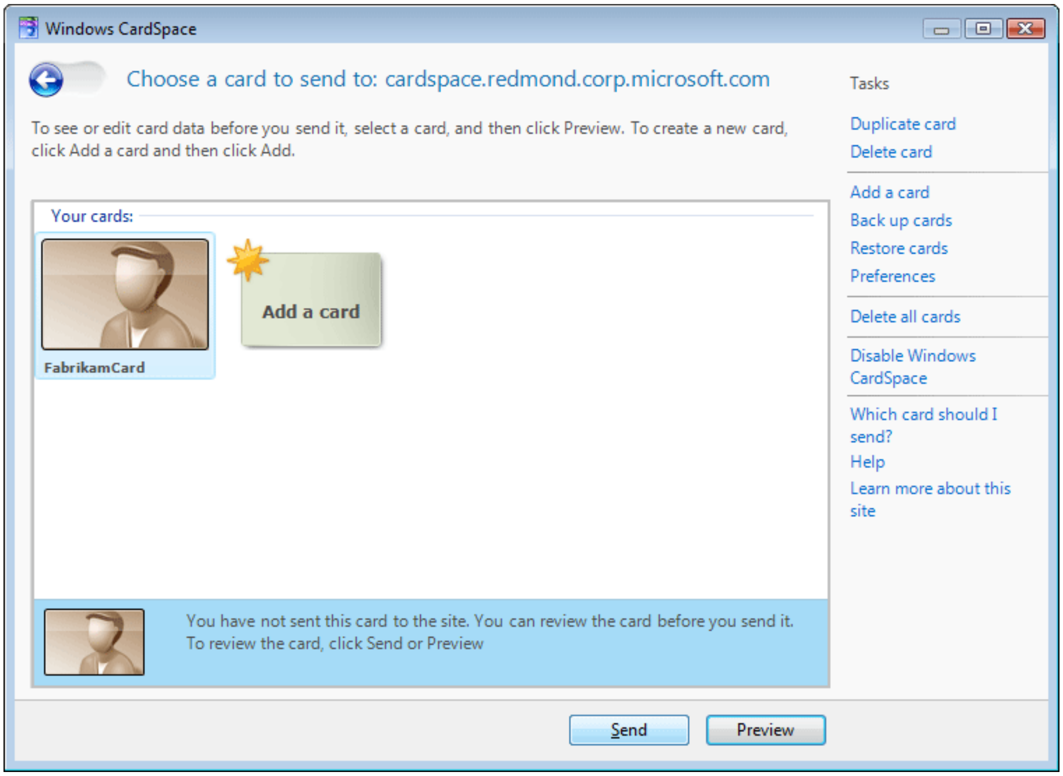
You can also download **managed** cards from organizations like banks, associations, and businesses. When you want to prove something about yourself to a website, for instance “I am a member of club X” or “I work for company Y”, show that website a managed card. A managed card is stored on your computer, but the information it conveys is not.

Using software like **Windows CardSpace**, you control which cards you get and how you use them. There is no centralized service and no one tracking how or when you use your cards – that information is between you, the card issuer, and the websites where you share your cards.

Does my system support Information Cards

A quick check of your system indicates that your system already supports Information Cards.

Clicking the sign-up button invokes the client's Identity Selector, such as the Windows CardSpace Identity Selector, which is depicted in the following figure.

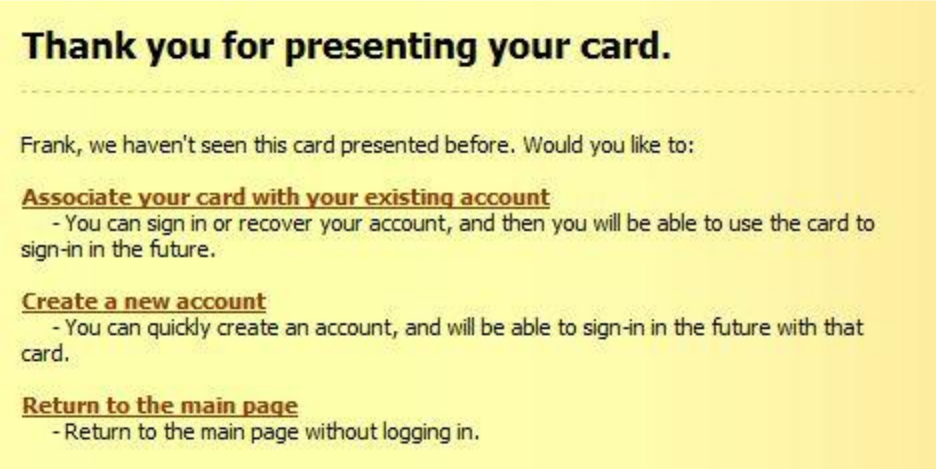


To see or edit card data before you send it, select a card, and then click Preview. To create a new card, click Add a card and then click Add.

You have not sent this card to the site. You can review the card before you send it. To review the card, click Send or Preview

The Identity Selector provides the user with the ability to select a card that they already have or to create another Personal Information Card that represents their identity. The user selects a card, and the user's personal identity provider issues a security token—which is signed with the private key of the user's card—that contains claims about the user's identity. The Web site receives, verifies, and deserializes this token. The Web site processes the identity claims that are stored in the token to associate them with an account and then authorize or deny access to the site.

When the Web site receives this token for signing up a new account, developers should provide UI that enables the user to determine whether to associate the token with an existing account on the Web site, create a new account based on the claims that are presented in the token, or ignore the token and return the user to the sign-up page. One potential UI for this logic is displayed in the following figure.



Thank you for presenting your card.

Frank, we haven't seen this card presented before. Would you like to:

Associate your card with your existing account
- You can sign in or recover your account, and then you will be able to use the card to sign-in in the future.

Create a new account
- You can quickly create an account, and will be able to sign-in in the future with that card.

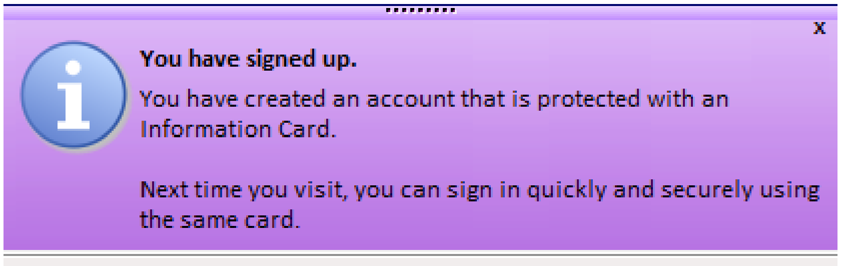
Return to the main page
- Return to the main page without logging in.

If the user chooses to create a new account, the site can simply request any remaining account details. It may be able to determine the values for some or all of those details by examining the claims that are presented in the user's Information Card.

As an alternative, the user may simply choose to associate the card with an existing account. For more information about this scenario, see "Enabling Authentication with Information Cards and Passwords."

A user may also lose their Information Card and need to use a new one with the same account. For more information about this scenario, see "Enabling Information Card Recovery."

After the user's card is associated with an account, the Web site should inform the user that they can log in to the site with it again in the future, as shown in the following figure.



You have signed up.

You have created an account that is protected with an Information Card.

Next time you visit, you can sign in quickly and securely using the same card.

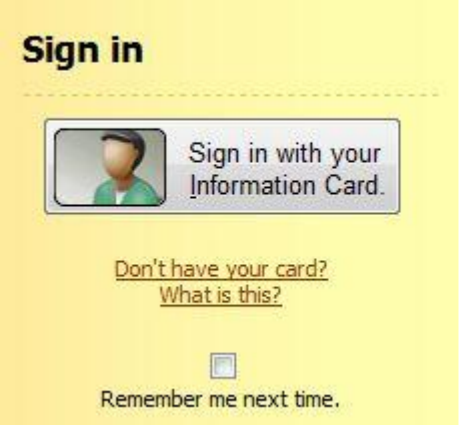
To add this sign-up experience to a Web site, perform a few simple tasks. First, add the Information Card UI elements to the site's markup. For the sign-up page, this normally takes the form of a standard button indicating support for Information Cards, along with supporting text explaining its use. When the user clicks the button, client-side code invokes the Identity Selector.

For more information about invoking the Identity Selector, see How to Use Windows CardSpace with Internet Explorer 7.0 (http://go.microsoft.com/fwlink/?LinkId=87317). For more information about the standard graphic elements that are available to Web site developers implementing Information Card support, see the "Appendix".

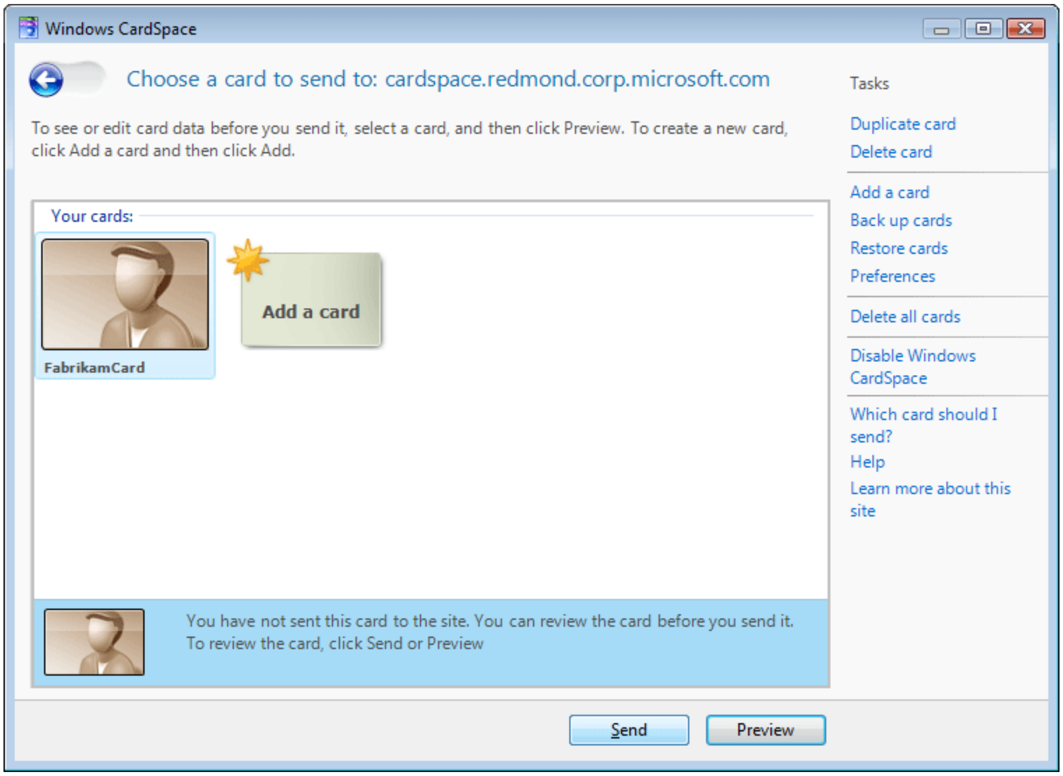
Enabling Information Card Sign-In

When users can sign up for access to a Web site with their Information Cards, they can use those cards to sign in to the site as well.

When they visit the site, users see the now-familiar sign-in page, as shown in the following figure.



Clicking the Information Card button triggers the client computer's local Identity Selector. The following figure shows the Windows CardSpace Identity Selector as triggered through Internet Explorer 7.



Choose a card to send to: cardspace.redmond.corp.microsoft.com

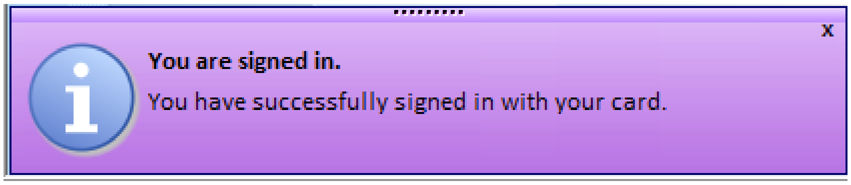
To see or edit card data before you send it, select a card, and then click Preview. To create a new card, click Add a card and then click Add.

You have not sent this card to the site. You can review the card before you send it. To review the card, click Send or Preview

When the user selects and submits their chosen card, the Web site receives the security token that is submitted by the client. The Web site decrypts the PPID claim and public key that is contained in the token. The Web site then looks up these items in the local Information Card database, determines which application account maps to those claims, and signs the user in to the appropriate account on the Web site.

Note:

User studies have shown that many users associate signing in with typing in a user name and password. With Information Cards, this does not happen. In fact, the sign-in process is seamless enough that some users may not realize that sign-in has completed successful. For this reason, you may want to notify the user that they have signed in successfully, if it is not otherwise apparent. An example notification is shown in the following figure.



You are signed in.

You have successfully signed in with your card.

Develop the markup and code for your preferred choice of sign-in reminder UI. Most of this markup and code is based on the UI that is shown and discussed in "Enabling Information Card Sign-Up." However, you must make some important choices.

The Information Card sign-in code, then, must trigger the invocation of the Identity Selector, and then process the user's security token, much as the sign-up page does. After the token is processed, the code then takes the user's PPID claim and public key signature and looks that user up in the local site's accounts table. After the user's account is identified, the user may be assigned session state (with a cookie or other preferred mechanism), and the user may go on to use the site.

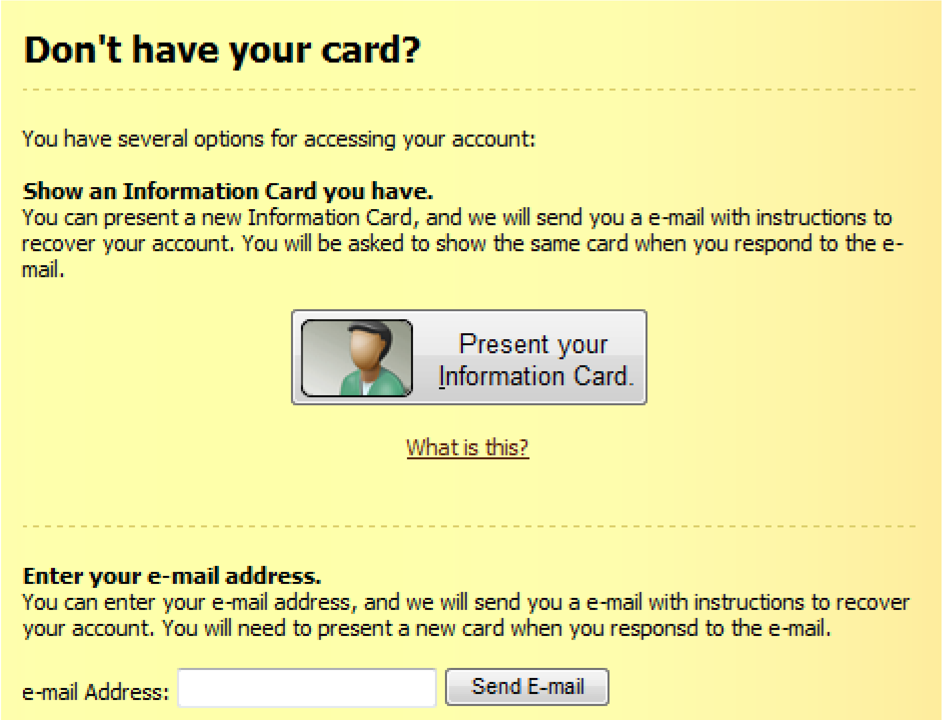
In the past, when a user first signs up to your site, you would gather required data about that user for your account database. With Information Cards, much of this information can be gathered as claims. However, you may no longer need to store this information in your account database. Instead, consider storing only essential user information in your database and continue to reacquire all other user data during subsequent sessions, as-needed.

Enabling Information Card Recovery

In much the same way that users sometimes forget their password, users may lose or misplace the Information Cards that they have used to sign in to Web sites. Cards may become lost as users move from computer to computer, as computers fail, or as computers are deleted.

E-mail verification is a simple way for a Web site to enable a user to recover their account. To take advantage of e-mail verification, validation of a user's e-mail address must take place during the creation of the user's account. This process normally involves requesting an e-mail address from the user during signup and then sending that address an authorization URL that the user must visit before their account becomes active.

The recovery process begins when the user notifies the Web site that they have lost their card through a link such as the "Don't have your card?" link in the following figure.



Don't have your card?

You have several options for accessing your account:

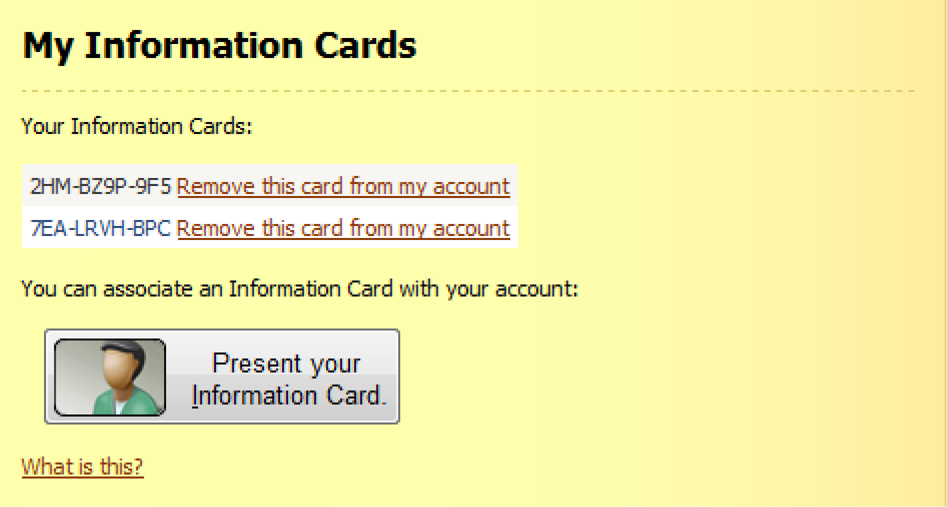
Show an Information Card you have.
You can present a new Information Card, and we will send you a e-mail with instructions to recover your account. You will be asked to show the same card when you respond to the e-mail.

Enter your e-mail address.
You can enter your e-mail address, and we will send you a e-mail with instructions to recover your account. You will need to present a new card when you responsd to the e-mail.

e-mail Address:

The Web site next displays a page asking the user to enter their e-mail address. The site then looks up the user's account using that address as a key. When an account is found, the site generates a unique identification code and sends it by e-mail to the user's address. After the user receives this code and enters it at the Web site, the site triggers the user's Identity Selector to generate a new card and associate it with their account.

At this point, the user has multiple Information Cards associated with their account. The Web site must be able to enumerate all the Information Cards that are associated with the account and display them as part of its account management page, providing the user with the option to remove any lost or unwanted cards from the account. The PPID field that is stored in the site's card database provides a good reference for the user to distinguish between their cards. The following figure shows an example of such a Web page.



My Information Cards

Your Information Cards:

2HM-BZ9P-9F5 Remove this card from my account

7EA-LRVH-BPC Remove this card from my account

You can associate an Information Card with your account:

What is this?

The ability to associate multiple Information Cards with a single site account provides a great deal of flexibility for users. For example, users can generate Information Cards on different computers and still preserve the quality of the Information Card sign-in experience on each computer.

Note:

As an alternative, sites may choose to allow only a single Information Card to be associated with each account. In this case, the lost card experience automatically removes the old card association, in a manner that is similar to how lost password experiences reset the account password. To log in from multiple computers, users must have copies of the Information Card that is associated with the account on those computers. This can be accomplished in Windows CardSpace by means of the backup card/restore card functionality.

Detecting Client Support

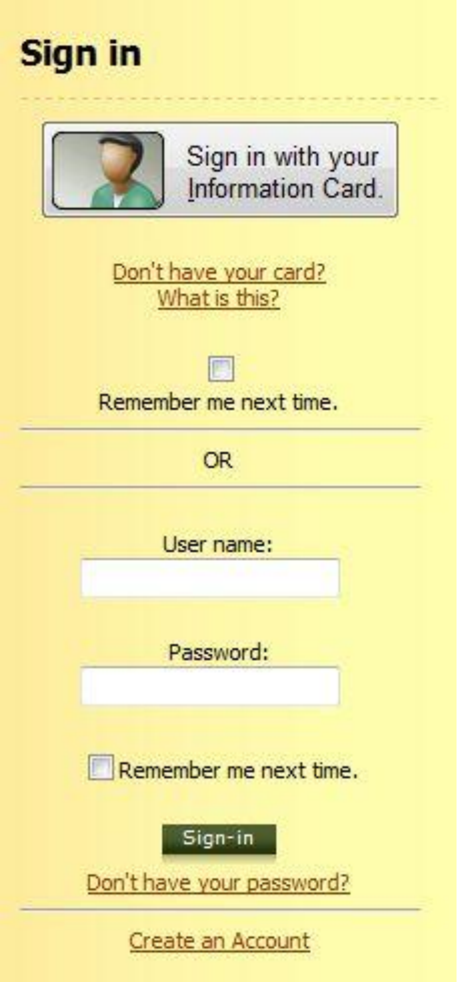
The Web code for embedding the Information Card UI should also attempt to detect if the user's current browser and operating system support Information Cards. Web site developers can use the client-side script in the Information Card Kit for HTML (http://go.microsoft.com/fwlink/?LinkId=89182) to detect Information Card support.

If the user’s current browser does not support Information Cards, the Web site can simply direct the user to Get Started with CardSpace (http://go.microsoft.com/fwlink/?LinkID=87450), which is maintained with current instructions for installing Information Card support as it becomes more widely available.

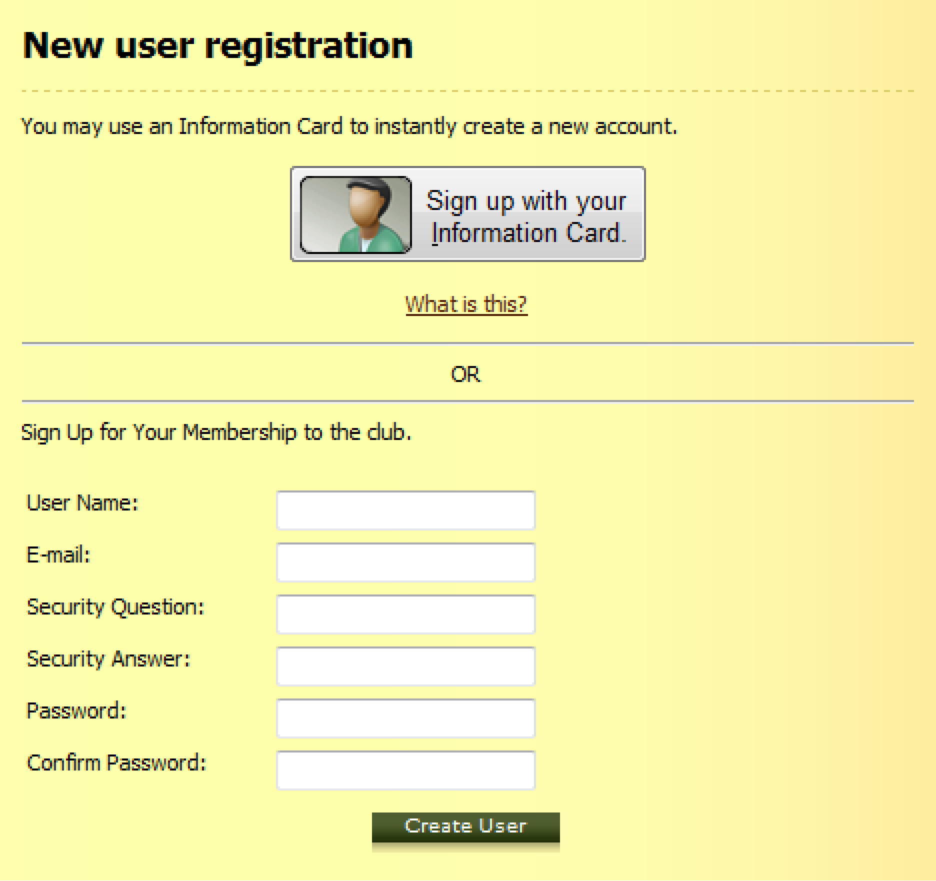
Information Cards and Passwords

This document focuses on Web sites that rely solely on Information Card authentication. However, operators of Web sites may want to support multiple authentication mechanisms because password authentication will remain popular until Information Card authentication becomes ubiquitous. A Web site that supports both Information Cards and password authentication gives its users more flexibility for card recovery and for signing in from multiple locations, some of which may not have Identity Selectors.

When a user visits a Web site that supports both Information Card authentication and forms-based password authentication, they see both options in the sign-in page, as in the example in the following figure.



If the user wants to sign up for the site, they are presented with the option to create an account either with a user name and password or with an Information Card. The following figure depicts one technique for prompting the user for this information.



New user registration

You may use an Information Card to instantly create a new account.

Sign Up for Your Membership to the club.

A number of different scenarios are possible at this point:

- A user can sign up by associating an Information Card with an account on the site and then also enable a password. This password can be used for card recovery (in combination with the e-mail-based recovery system that is described in "[Enabling Information Card Recovery]") if the user loses their Information Card, for sign-in when the user cannot use Information Cards, or both.

  Note:

  You may want to design your application to demand answers to additional security verification questions when a user attempts to sign in to the site using a password instead of an Information Card.

- As an alternative, a user can sign up using a user name and password without enabling an Information Card. The user can associate an Information Card with this account at a later date. Again, you may want to require additional verification questions for password-based sign-in.

Note:

It is important to recognize that the user is *not* required to use both an Information Card and a password. The two authentication techniques are distinct. Users can access their Web site account using either an Information Card or a user name and password combination.

The scenarios that are described in this document enable you to provide users of your site with the flexibility to use Information Cards for registration and sign-in, either in conjunction with or as a replacement for password authentication. Information Card support detection, Information Card recovery, and association with previously existing application accounts can be provided with minimal changes to the architecture of a Web site. With these changes in place, users of Windows CardSpace or other Identity Selectors can take advantage of the speed, flexibility, and security of Information Card authentication.

Acknowledgements

Substantial technical contributions to this document were made by Keith Ballinger, Mike Jones, Stuart Kwan, Curt Smith, Derek Del Conte, and Rob Franco. Jim Becker served as editor, with additional edits by John Andrilla.

Appendix

The following sections explain how to gain access to the elements of the standard Information Card UI look and feel (“Iconography”), enhance the accessibility of a site using Information Cards ("Accessibility"), provide links to more information about Information Cards and Windows CardSpace (“Related Links”), and define key terms (“Glossary”).

Iconography

Users will be unfamiliar with the Information Card sign-in interface for the short-term future. A consistent look and feel for the UI will help users instantly recognize that the site they are using supports Information Cards. To help Web site designers achieve this consistency, Microsoft plans to create a set of images that any site can use royalty free.

We expect that the final recommended Information Card icon image will have a 10:7 width-to-height ratio. Please plan to include it when it becomes available as you design your user experience. We have used the image below as a placeholder for the actual image, to illustrate the role that an Information Card icon will play in the user experience.

Accessibility

You should provide for accessibility in the elements of your Web page, including the graphic elements and forms related to Information Card sign-in and sign-up.

- Each interactive element, such as buttons, should provide keyboard accelerators to activate their functionality. It's recommended that Web sites use the letter "i" as the accelerator key to invoke the selector.
- Test the tab-order of the form elements on all of your pages to make certain it's logical and intuitive
- Provide ALT text for every graphic element on the page, to assist screen readers in describing their functionality

Related Links

To learn more about using Information Cards at web sites, see A Guide to Supporting Information Cards within Web Applications and Browsers as of the Information Card Profile V1.0, December 2006 (http://go.microsoft.com/fwlink/?LinkID=88956).

To learn more about the specifics of the Information Card protocol, see A Technical Reference for the Information Card Profile V1.0 (http://go.microsoft.com/fwlink/?LinkId=87444).

To examine the common, interoperable system architecture using Information Cards, see A Guide to Interoperating with the Information Card Profile V1.0 (http://go.microsoft.com/fwlink/?LinkId=87446).

You can find more information about the Microsoft Information Card implementation, Windows CardSpace, as well as the Microsoft vision for an Identity Metasystem, in Introducing Windows CardSpace (http://go.microsoft.com/fwlink/?LinkId=87449).

To stay up to date with news, documentation, and samples for the Windows platform, see the Windows CardSpace home page, Get Started with CardSpace (http://go.microsoft.com/fwlink/?LinkId=87450), and the Windows CardSpace documentation home page on MSDN, Using CardSpace in Windows Communication Foundation (http://go.microsoft.com/fwlink/?LinkId=87451).

Developers can build ASP.NET applications that accept Information Cards with the Information Card Kit for ASP.NET (http://go.microsoft.com/fwlink/?LinkId=89183).

For client-side scripting support, use the Information Card Kit for HTML (http://go.microsoft.com/fwlink/?LinkId=89182).

Glossary

Browser

A program for viewing downloaded HTML pages. Web browsers that support Windows CardSpace include Microsoft Internet Explorer 7 and Mozilla FireFox 1.5 and 2.0 (with an optional plug-in).

Claim

A claim is a statement about the Subject of the claim, which is made by an Identity Provider (such as name, date of birth, e-mail address, or shoe size).

Identity Provider

An organization that acts as a provider of identity information. Identity providers provision Managed Information Cards for users, and they supply the identity claims that are contained in those Managed Information Cards. See Information Card, Managed Information Card.

Information Card

A representation of identity that is assured by a particular party and delivered in the form of an encrypted token. When it is decrypted, this XML-formatted token contains a set of identity claims and a public key for validating the token's signature.

Identity Selector

A security-hardened UI that appears when a user needs to choose an Information Card to send to a Relying Party. Identity Selectors provide functionality for examining a site's privacy policy, generating a personal Information Card, and selecting and sending an appropriate Information Card (either Personal or Managed) to a Web site.

Managed Information Card

An Information Card that is provided by an external Identity Provider, such as a bank or workplace. With Managed Information Cards, claims data is stored by the Identity Provider, unlike a personal card. See Information Card, Personal

Card.

Personal Information Card

An Information Card that is created by a user that makes self-asserted claims about that user. All identity data is created by the user and maintained locally in an encrypted store. In the case of Microsoft Windows, Windows CardSpace is responsible for this store. See Information Card. Personal Information Cards as also known as Self-Issued Information Cards.

PPID

Personal Private Identifier. PPIDs are generated dynamically when Information Cards are first issued to each Web site, and they are tied to the public key of the issuing security token service (STS) and the public key of the relying party. This helps protect the user's identity because relying parties cannot compare PPIDs while trying to identify users.

Therefore, PPIDs that are presented by clients to the same relying party differ based on the STS that issued the token. In addition, PPIDs that are presented by clients to different relying parties based on the same STS also differ.

Relying Party

A Web site or service that requests an Information Card.

Self-Issued Information Card

See Personal Information Card.

Subject

The entity about which the Information Card makes its claims. The subject of an Information Card is normally the user who holds the card.

Windows CardSpace

Windows CardSpace is the Microsoft implementation of an Identity Selector for the Windows platform. It provides a user interface that users can use to generate, select, and submit Information Cards to Relying Parties. See Identity Selector.