

**Microsoft**

# **Patterns for Supporting Information Cards at Web Sites: Personal Cards for Sign-up and Sign-In**

---

Microsoft Corporation

Published: August 2007

Authors: Keith Ballinger, 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.

**Microsoft**

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2007 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows Server, Windows Vista, Windows CardSpace, and ASP.NET are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

# Contents

---

Supporting Information Cards on Web Sites .....	5
Implementing Information Card Support .....	8
Enabling Information Card Sign-Up .....	9
Enabling Information Card Sign-In .....	14
Enabling Information Card Recovery .....	16
Detecting Client Support .....	18
Information Cards and Passwords .....	19
Summary .....	22
Appendix.....	22



# 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. The traditional method for users to identify themselves to a Web site—password authentication—has a number of well-known flaws. Web site developers can address many of these issues by supporting Information Cards.

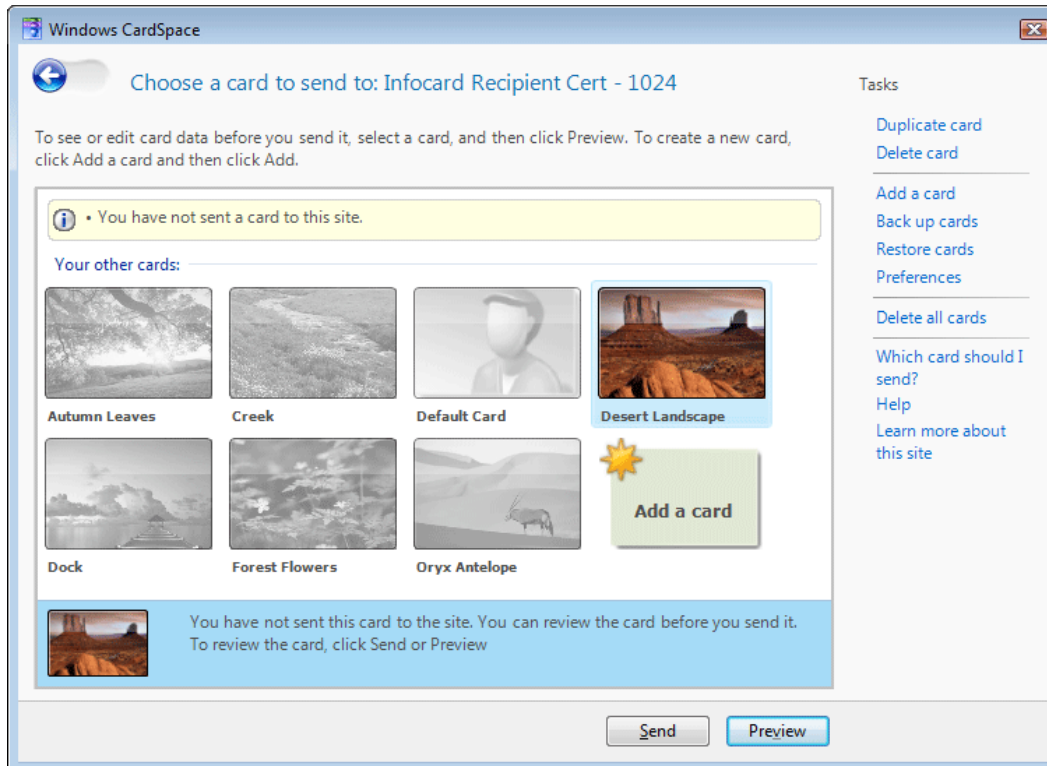
Information Cards provide a visual representation for digital identities. The user can use Information Cards to select which digital identities to employ at different Web sites. Information Cards provide users with a simpler and safer experience that is similar to the card experience that they have in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

After meeting a set of basic prerequisites, Web site developers can support account sign up and sign in using Information Cards. Web sites can also support the use of Information Cards along with traditional password authentication. These distinct techniques can complement one another or provide alternative authentication options for users.

## 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 employee ID cards.

Information Cards are managed on client computers by a software component called an Identity Selector. An Identity Selector is a 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.



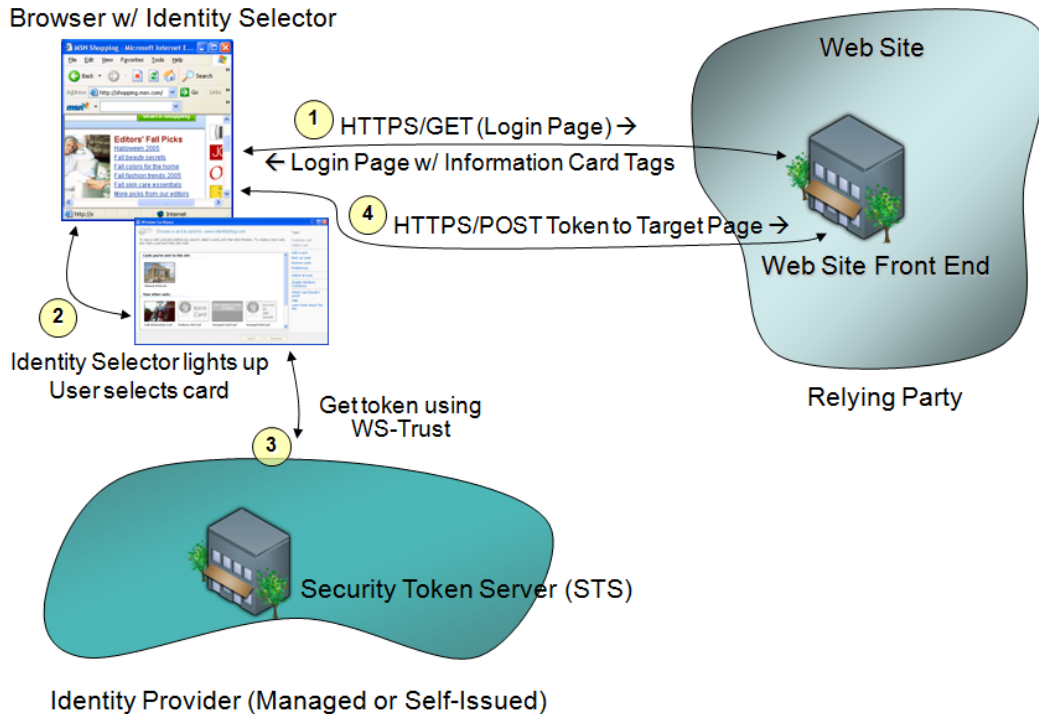
Each Information Card represents one or more claims about a user's identity. These claims can be as simple as a person's name, or they can include a wider range of information. Web sites can consume these claims for the purposes of sign-in and sign-up, as well as for other purposes. For more information 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 five participants:

- The user, who has a collection of digital identities represented by Information Cards.
- Identity Providers, which issue digital identities that are represented by Information Cards. An Information Card points to a web service at an Identity Provider that issues security tokens. Security tokens are XML documents that contain claims. Security tokens are digitally signed by the identity provider to assure their authenticity.
- Identity Selectors, which hold the user's collection of Information Cards, enables the user to pick a card for use at a web site, and retrieves a security token from the associated Identity Provider when the user picks a card.
- Web browsers, which call Identity Selectors to request a security token, and post the returned token to a web site.

- Web sites, which accept the claims that the user presents through an Information Card. A web site receives, processes, and verifies security tokens, then uses the claims in the security token to sign the user in, or sign them up to the site.

#### Browser w/ Identity Selector



For example, a company may issue Information Cards for its employees or for customers.

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.

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, employee ID card, 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 focuses on Personal Information Cards and does not cover advanced scenarios, such as age verification or online payment solutions.

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>).

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.

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.

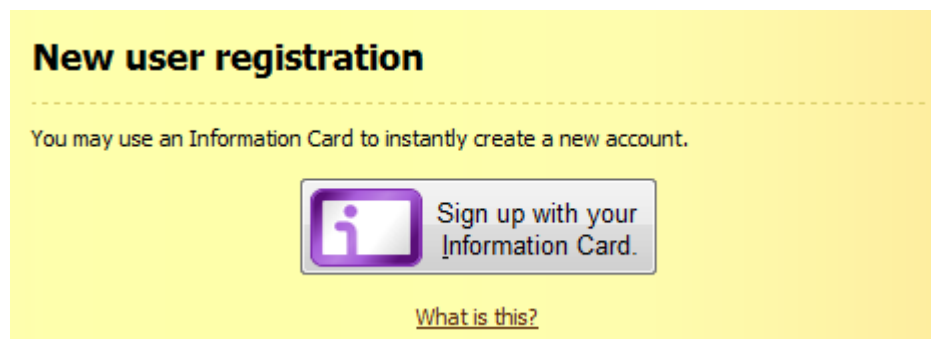
Some certification authorities are issuing a new class of SSL certificate, known as an Extended Validation (EV) certificate. EV certificates are issued under more stringent identification guidelines. However, Identity Selectors are able to make stronger statements about the identity of a site that is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

- Configure time synchronization. Security tokens include time-stamped validity intervals to protect against man-in-the-middle attacks. It is important for the clock at a Web site to be synchronized with the clock at an identity provider, where security tokens are generated. 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. As with most Websites, you can present them with a link to a sign-up page. The sign-up page can explain to the user that they simply need to present a card to sign-up with the site.



## Claims Used for Sign-Up

A button on the Web page can be used to invoke the Information Card selector and acquire specific information (called claims) from the user before sending these claims to the Web site. In this example, when the user signs up with their card, the Website requests three claims.

Requested Claim	Description
PPID	A Private Personal Identifier. This string is unique value for each pairing of a card and Web site's SSL certificate.

First Name	The user's first name.
Last Name	The user's last name.
E-mail Address	The e-mail address of the user.

One other value is also received by the Web site: the public portion of the key that signed the token containing these claims. With Personal Cards, this key is cryptographically secured at the user's computer.

Each of these values, along with the public key, can be stored in the Web site's database and used to authenticate a user upon subsequent login. Typically, a combination of the PPID and the public key will be used for the actual authentication string.

To create a button that invokes an Information Card selector, you can use JavaScript and the HTML OBJECT tag. The type attribute of the OBJECT tag must be "application/x-informationCard". The PARAM child element of type "requiredClaims" is used with a value of the claims that are requested. The following snippet illustrates this (URIs are edited for clarity.)

```
<OBJECT
  type="application/x-informationCard"
  name="icard">
<PARAM
  Name="issuer"
  Value="http://.../self">
<PARAM
  Name="requiredClaims"
  Value=
    "http://.../emailaddress
    http://.../givenname
    http://.../surname
    http://.../personalprivateidentifier">
</OBJECT>
```

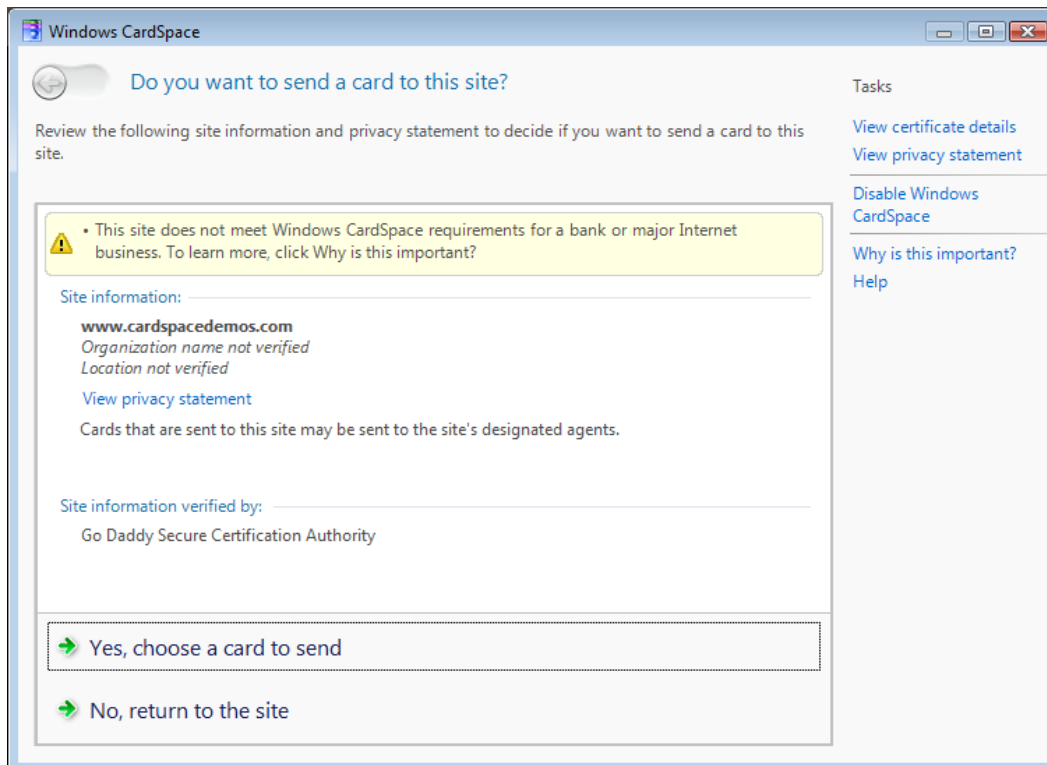
Next, when the button is clicked, the OBJECT's **value** property can be accessed from script. This will invoke the selector. The values inside the tag, such as the required claims, will be conveyed to the invoked selector. When the property is returned, it will be an encrypted and signed security token containing the requested claims. At this point, you can use your Web development technology (ASP.NET, PHP, JSP, etc) to post this token back to your server and process the token accordingly.

For more information about the HTML markup and client-side code to invoke the Identity Selector, see “How to Use Windows CardSpace with Internet Explorer 7.0” (<http://go.microsoft.com/fwlink/?LinkId=87317>). You can use the “Information Card Kit for HTML” (<http://go.microsoft.com/fwlink/?LinkId=89182>) to add client-side Information Card functionality to your Web site.

For more information about the standard graphic elements that are available to Web site developers implementing Information Card support, see the "[Appendix](#)".

## User Experience at Sign-up

When the user clicks the button and submits a card to the Web site for the first time, they will see the following screen, which explains the site’s details and allows them to view the Website’s privacy statement. Additionally, they can elect to not send a card.



 **Note:**

As seen in the above screenshot, users are informed when a Website is not a bank or major Internet business. This text appears when a site does not use EV (Extended Verification) SSL certificates.

When a user decides to submit a card for sign-up, they may decide (or need) to create a card for this site. The fields that are required will be highlighted in red.

Windows CardSpace

← Edit a new card

Tasks  
What data should I include on my card?  
Help

The details of this personal card indicate what data will be sent to the site. You can change the data, name, and picture for this card.

Card properties:

Card Name: My Card

Image File: Choose Picture...

Personal Card

Card data that will be sent to this site:

Fields marked with an asterisk (\*) are required

\* First Name: Jeff

\* Last Name: Price

\* Email Address: Jeff.Price@contoso.com

Card data that will not be sent:

Street: Not specified

City: Not specified

State: Not specified

Postal Code: Not specified

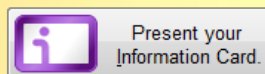
Save Cancel

When the user is finished creating the card, they can submit it and an account can be created. However, it may be a good idea to use e-mail verification before activating the account. The e-mail claim that was required earlier can be used to send an email. The user can be alerted to this.

**An e-mail has been sent to your account at Jeff\_Price@contoso.com.  
Please follow the instructions in the message to access your account.**

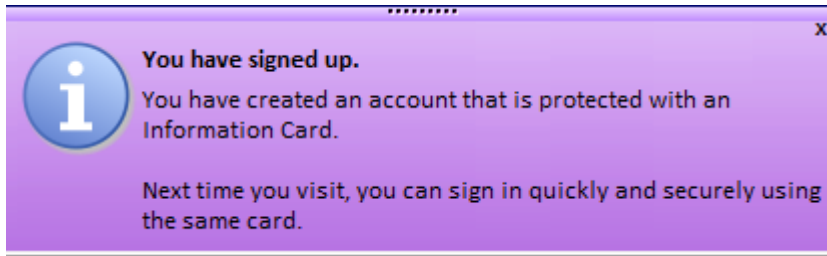
Once the user clicks on the link sent to their email, a secondary authentication can be performed to ensure that the email was not intercepted. Specifically, the card used to create the account can be asked for again.

In order to validate that you both the person that requested access, and that you do control the email address you indicated, the same Information Card must be presented again.



[Why do I have to show my card again?](#)

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



## Alternative Sign-Up Processes

You can also sign a user up through the sign-in process. The user may try to sign into the site with a card, mistakenly thinking that they have already signed-up.



When the Web site receives a token that contains claims that do not match an existing 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.

A user may also lose their Information Card and need to associate a new card with an existing account. For more information about this scenario, see "[Enabling Information Card Recovery](#)."

#### **Note:**

Information Cards do not obviate the need for CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) at sign-up. An Information card is not sufficient proof that a human has registered at a site.

## Enabling Information Card Sign-In

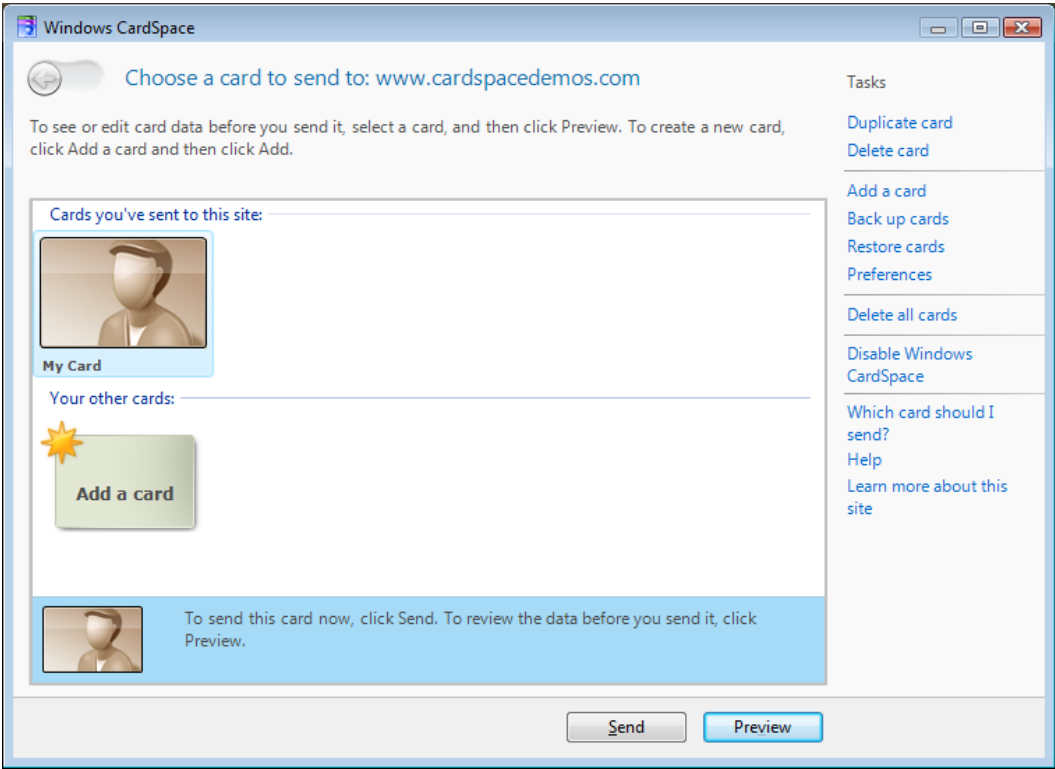
---

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 sign-in page, as shown in the following figure. As this figure shows, Information Card sign in can also work with persistent sessions, as modeled with the "Remember me next time" text. This is not required or suggested in all cases.



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



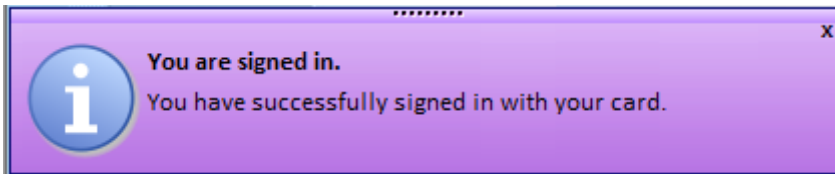
When the user selects and submits their chosen card, the Web site receives the security token that is submitted by the client. The Web site decrypts the PPID (Personal Private Identifier) claim and public key that is contained in the token. The Web site then looks up

these items in the local user account database, determines which application account maps to those claims, and signs the user in to the appropriate account on the Web site.

 **Note:**

A Personal Private Identifier (PPID) is generated dynamically and tied to the public key of the Web site's SSL certificate. It is unique to each Information Card and user. For more information on the PPID claim, see the Information Card Technical Reference 1.0 (<http://download.microsoft.com/download/1/1/a/11ac6505-e4c0-4e05-987c-6f1d31855cd2/Identity-Selector-Interop-Profile-v1.pdf>).

Many users associate signing in with typing in a user name and password. With Information Cards, the sign-in process is so rapid and seamless that many users do not realize that sign-in has completed successfully. For this reason, you may decide to notify the user that they have signed in successfully. An example is shown in the following figure.



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. For example, cards may become lost as users move from computer to computer.


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 sign-up and then sending that address an email containing 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.

 Present your Information Card.

[What is this?](#)

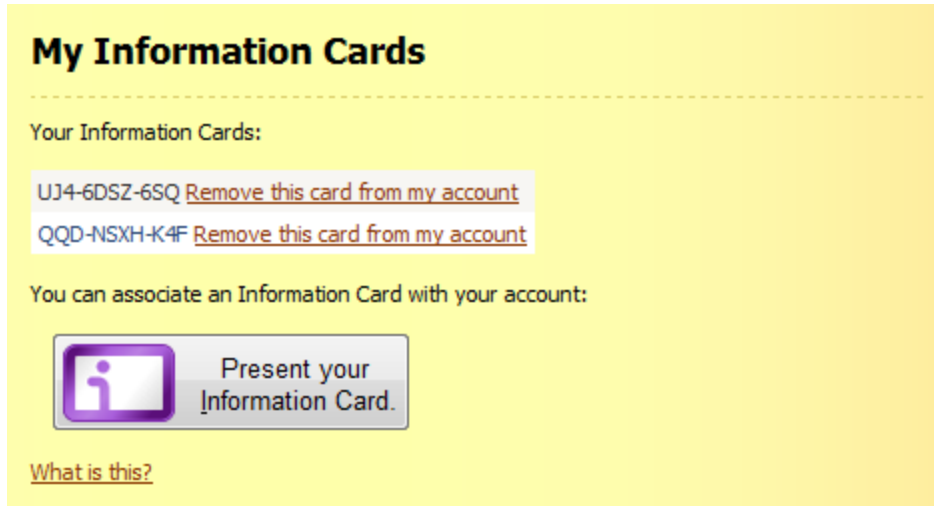
**Enter your e-mail address.**  
You can enter your e-mail address, and we will send you a e-mail with instructions to recover your account. You will need to present a new card when you respond to the e-mail.

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 request a 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.



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 can 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 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

## Sign in



Sign in with your  
Information Card.

[Why can't I use this?](#)

19

becomes more widely available. This detection can occur during the rendering of any Web page that includes an Information Card button, as the following figure shows.

## 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. 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 computers, 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.

## Sign in

---

 Sign in with your Information Card.

[Don't have your card?](#)  
[What is this?](#)

Remember me next time.

---

OR

---

User name:

Password:

Remember me next time.

[Don't have your password?](#)


---

[Create an Account](#)

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 with your Information Card.

[What is this?](#)

---

OR

---

Sign Up for Your Membership to the club.

User Name:

E-mail:

Security Question:

Security Answer:

Password:

Confirm Password:

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.

## Summary

---

The scenarios that are described in this document enable you to provide users of your site with the flexibility to use Information Cards for sign-up 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 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

A consistent look and feel for Information Card sign-in will help users instantly recognize that the site they are using supports Information Cards. To help Web site designers achieve this consistency, Microsoft has created a set of images that any site can use

royalty-free. You can download this package at:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=ce99e033-39a8-4bc5-9014-60ed0b560d0e&displaylang=en>



## 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

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>).

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>).

## 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).

See **Security Token**.

### Identity Provider

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

### Information Card

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 employee ID cards.

### Identity Selector

A 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 are also known as Self-Issued Information Cards.

**PPID**

The PPID claim for a user represents a unique identifier for that user at a given Web site that is different from all identifiers for that user at any other Web site. This helps protect the user's identity because relying parties cannot compare PPIDs while trying to identify users.

**Relying Party**

A Web site or service that requests an Information Card.

**Security Token**

A cryptographically signed XML document that contains a set of claims.

**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.