



# Célula Académica UABC-Live .net

Universidad Autónoma de Baja California  
Facultad de Ciencias Químicas e Ingeniería

<http://uabc-live-net.spaces.live.com/>

**Microsoft** | Partner Program

# Sesión No. 7

## CardSpace

### **Expositores:**

Blanca Patricia López Montes (**blanquita\_pretty@hotmail.com**)

**Fecha:** 17 de Marzo de 2007

# Índice

- Comprendiendo la identidad digital
- Describiendo la identidad digital
- Representando identidades digitales: Security Tokens
- Windows CardSpace y el metasisistema de identidad
- Windows CardSpace e Internet Explorer
- Aspectos importantes

# Comprendiendo la identidad digital

“¿Quién es usted?” es una pregunta simple, pero no tiene una respuesta simple. La manera en la que usted representa su identidad cambia a medida que se mueve por el mundo. Cuando presenta su pasaporte en un aeropuerto, es el ciudadano de algún país. Cuando muestra su licencia de conducir a un policía, es un conductor legal que reside en alguna localidad. Cuando usa su tarjeta de crédito para pagar algo, es un cliente con un número de cuenta en particular. Diferentes contextos requieren distintas identidades, cada una de las cuales es expresada de una manera diferente y contiene distinta información.

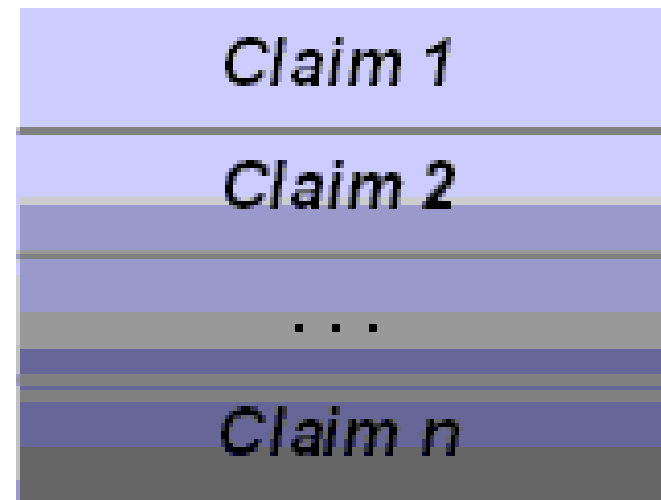
# Describiendo la identidad digital

Como las del mundo real, las identidades digitales vienen de distintas formas y tamaños. Seguramente usted tenga una cuenta de correo, por ejemplo, identificada por su dirección de e-mail. También puede tener identidades digitales con varias organizaciones comerciales, así como identidades para sitios. Cada una de ellas suele estar identificada por un nombre de usuario que usted definió. En el trabajo podría tener una identidad digital asignada por su empleador, identificada por su login de red. Esta identidad probablemente sea mantenida por algún servicio de directorio, como Active Directory, y hoy en día, generalmente es útil sólo dentro de los límites de la red de su compañía.

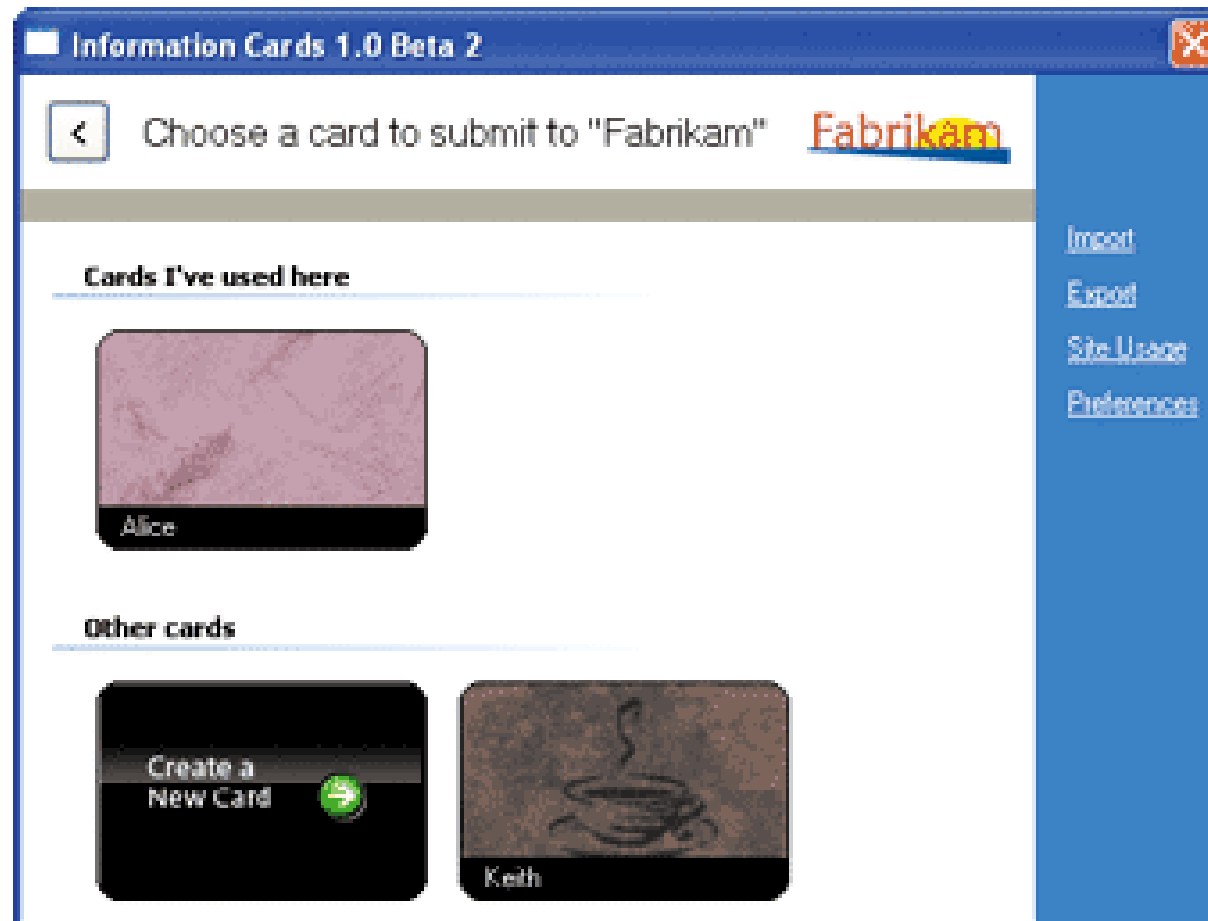
# Representando identidades digitales: Security Tokens

Todas las identidades digitales tienen un punto en común: cuando es transmitida en la red, cada identidad digital es representada por algún tipo de token de seguridad. Un token de seguridad es sólo un conjunto de bytes que expresa información sobre una identidad digital. Esta información consiste en uno o más *claims*, cada uno de los cuales contiene una parte de la información convenida sobre esta identidad. Un token de seguridad simple puede incluir un solo *claim* que contenga el nombre de usuario, mientras que uno más complejo puede incluir *claims* que contengan el nombre del usuario, apellido, dirección y más. Los tokens de seguridad por alguna identidad digital también podrían incluir *claims* que contengan información sensible, como números de tarjetas de crédito.

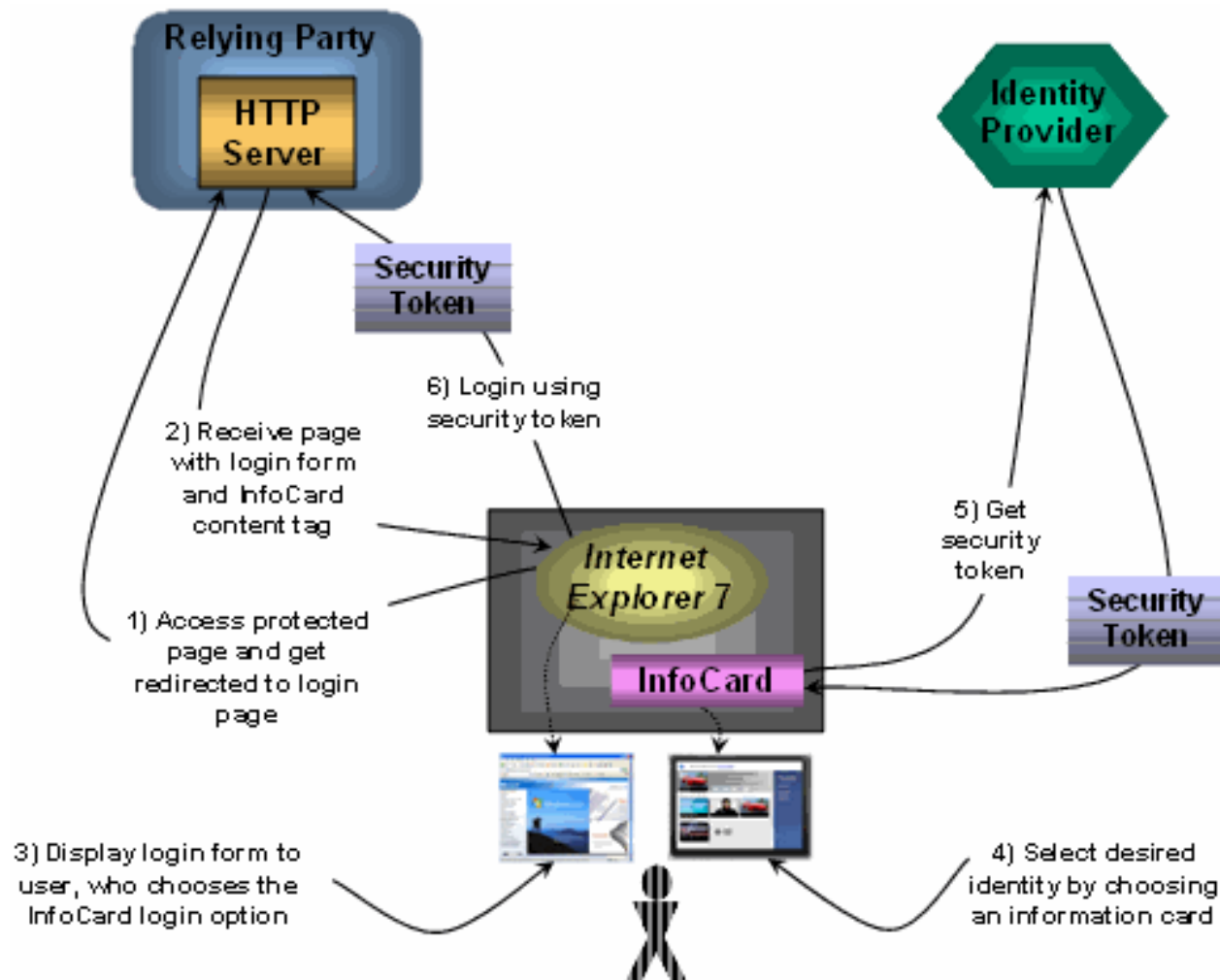
## Security Token



# Windows CardSpace y el metasisistema de identidad



# Windows CardSpace e Internet Explorer



# Windows CardSpace e Internet Explorer

- El proceso comienza cuando un usuario del navegador accede a una página protegida en un sitio web, como una página para comprar productos. En este punto, el sitio requiere que el usuario se loguee en este sitio, y por lo tanto el sitio redirecciona al navegador hacia su página de login.
- Este redireccionamiento hace que se mande un formulario de login desde el navegador. Este formulario le puede permitir al usuario loguearse en el sitio proporcionando su nombre de usuario y contraseña, pero si el sitio es compatible con CardSpace, la página que transporta el formulario también contendrá un **OBJECT** tag específico o una sintaxis XHTML.

# Windows CardSpace e Internet Explorer

- Si el usuario selecciona esta opción, IE 7 ejecutará un código identificado por el **OBJECT** tag o la sintaxis XHTML, que requerirá la implicación de CardSpace's en el proceso de login.
- La pantalla de CardSpace aparecerá, y el usuario podrá seleccionar una identidad.

# Windows CardSpace e Internet Explorer

- Hasta aquí, toda la comunicación con este sitio utilizó HTTP. Una vez que el usuario selecciona una identidad, sin embargo, CardSpace se contacta con el proveedor de la identidad usando WS-Trust, como es habitual, y obtiene el token de seguridad.
- Este token luego es enviado al sitio web usando HTTP POST como parte del proceso de login. La aplicación web puede usar el token para autenticar al usuario o para otro propósito.

# Aspectos importantes

**Hay cuatro aspectos importantes en esta tecnología:**

- Soporte a cualquier sistema de identidad digital.
- Control consistente de la identidad digital.
- Reemplazo del password basado en Web Login.
- Mejora en la confianza en la identidad de aplicaciones remotas.

# Aspectos importantes

## **Soporte a cualquier sistema de identidad digital**

- Los aspectos más importantes del proceso de un sistema que usa CardSpace incluyen:
  - Windows CardSpace y el metasisistema de identidad son enteramente agnósticos respecto al formato del token de seguridad que requiere un proveedor de identidad.
  - De hecho, CardSpace puede trabajar con cualquier sistema de identidades, usando cualquier tipo de token de seguridad, incluidos simples usernames, certificados X.509, tickets Kerberos, tokens SAML, o cualquier otro.
  - También permite conectar con cualquier otro sistema digital de identificación que aparezca en el futuro.

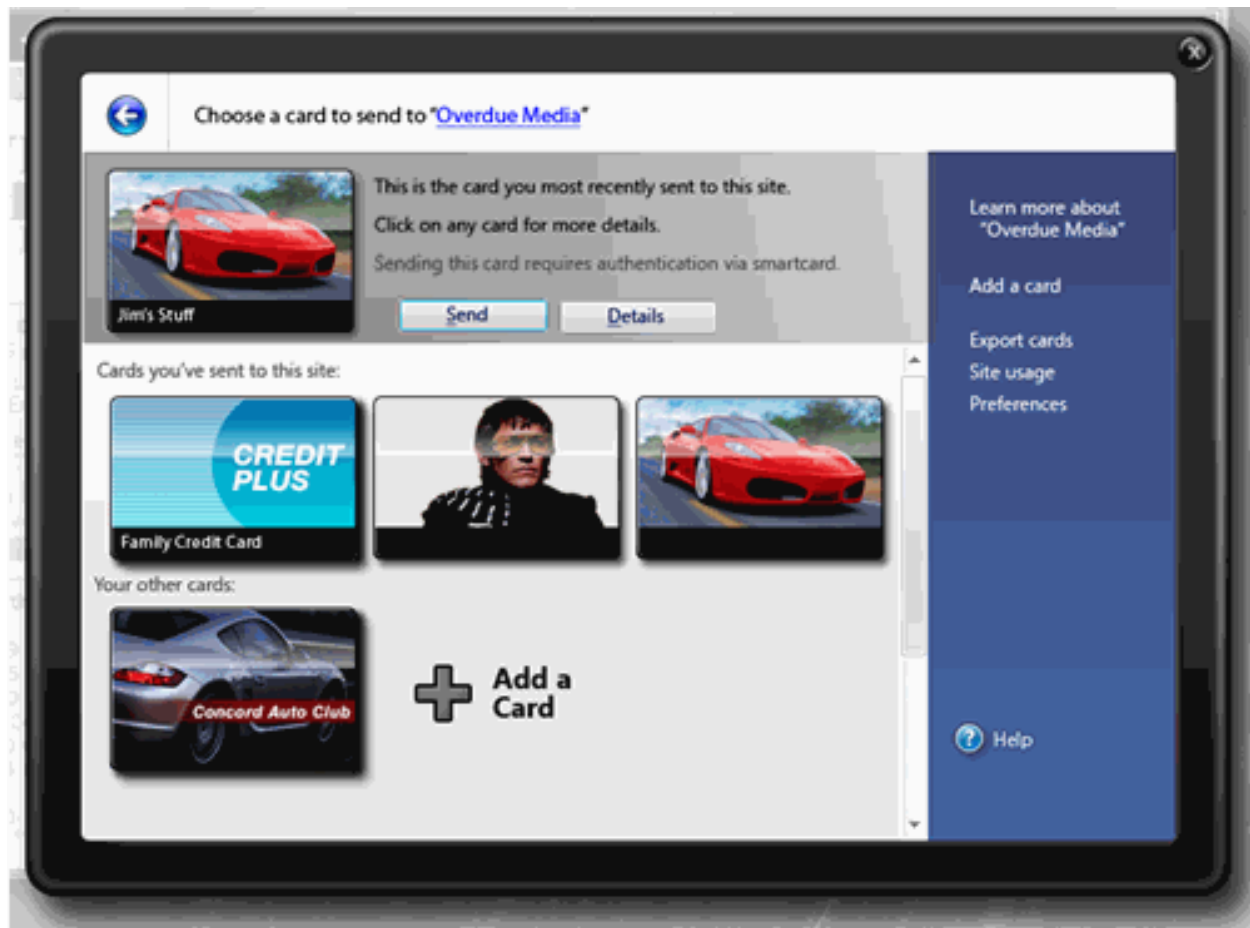
# Aspectos importantes

## Reemplazo del password basado en Web Login:

- Más que autenticación con usuarios y contraseñas, en un ambiente de confianza como un sitio web, la autenticación puede ser implementada con un token de seguridad.
- Por ejemplo, una compañía que disponga de una familia de sitios web puede ofrecer un proveedor de identidades, corriendo en cualquier máquina y accesible a cualquier cliente, que sea capaz de publicar tokens que son aceptados por esta familia de sitios.
- Esto minimiza el uso de passwords, y es una opción en la que se puede implementar CardSpace.

# Aspectos importantes

Control consistente de la identidad digital.



# Aspectos importantes

- Mejora en la confianza en la identidad de aplicaciones remotas.





# CardSpace con Internet Explorer 7.0



# Índice

- Introducción
- Ejemplo
- Procesar token de información

# Introducción

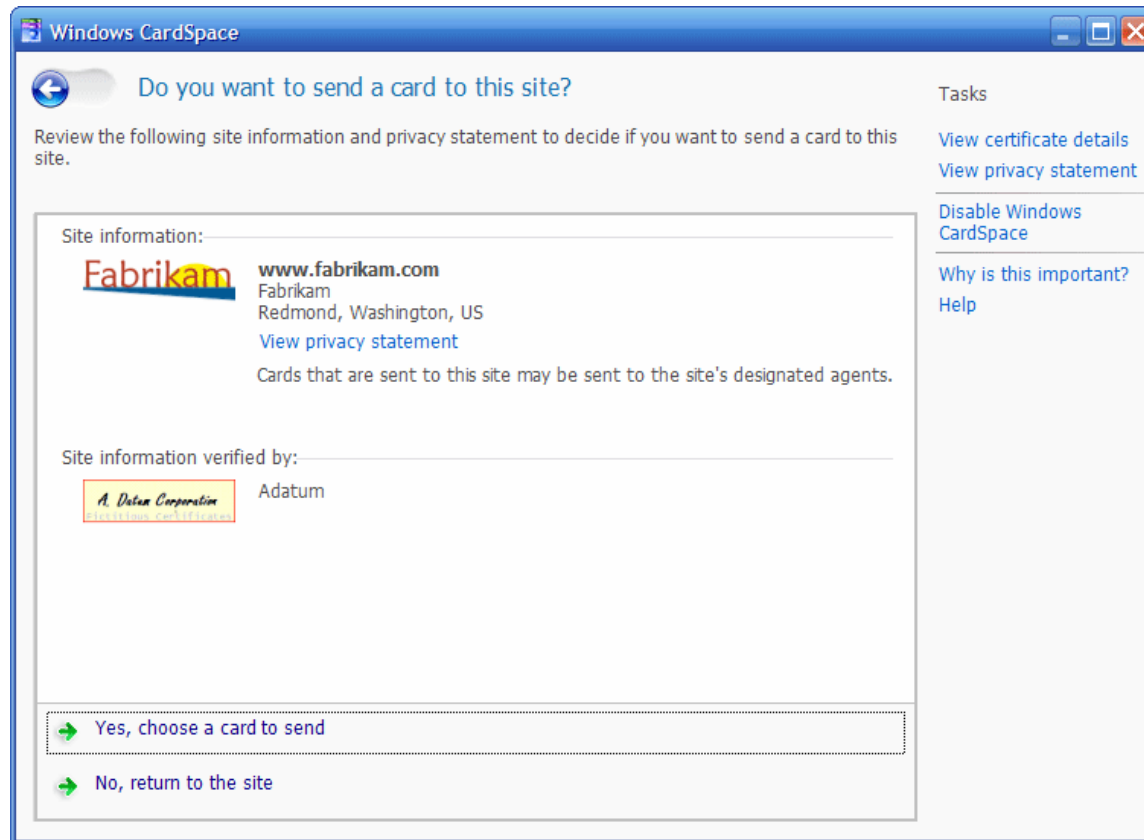
- Windows CardSpace provee a los usuarios la habilidad de manejar sus identidades digitales.
- Con Internet Explorer 7.0, los sitios web pueden hacer la petición de una identidad digital al usuario.
- El siguiente ejemplo demuestra los pasos para aceptar identidades usando CardSpace e Internet Explorer 7.0.

# Ejemplo

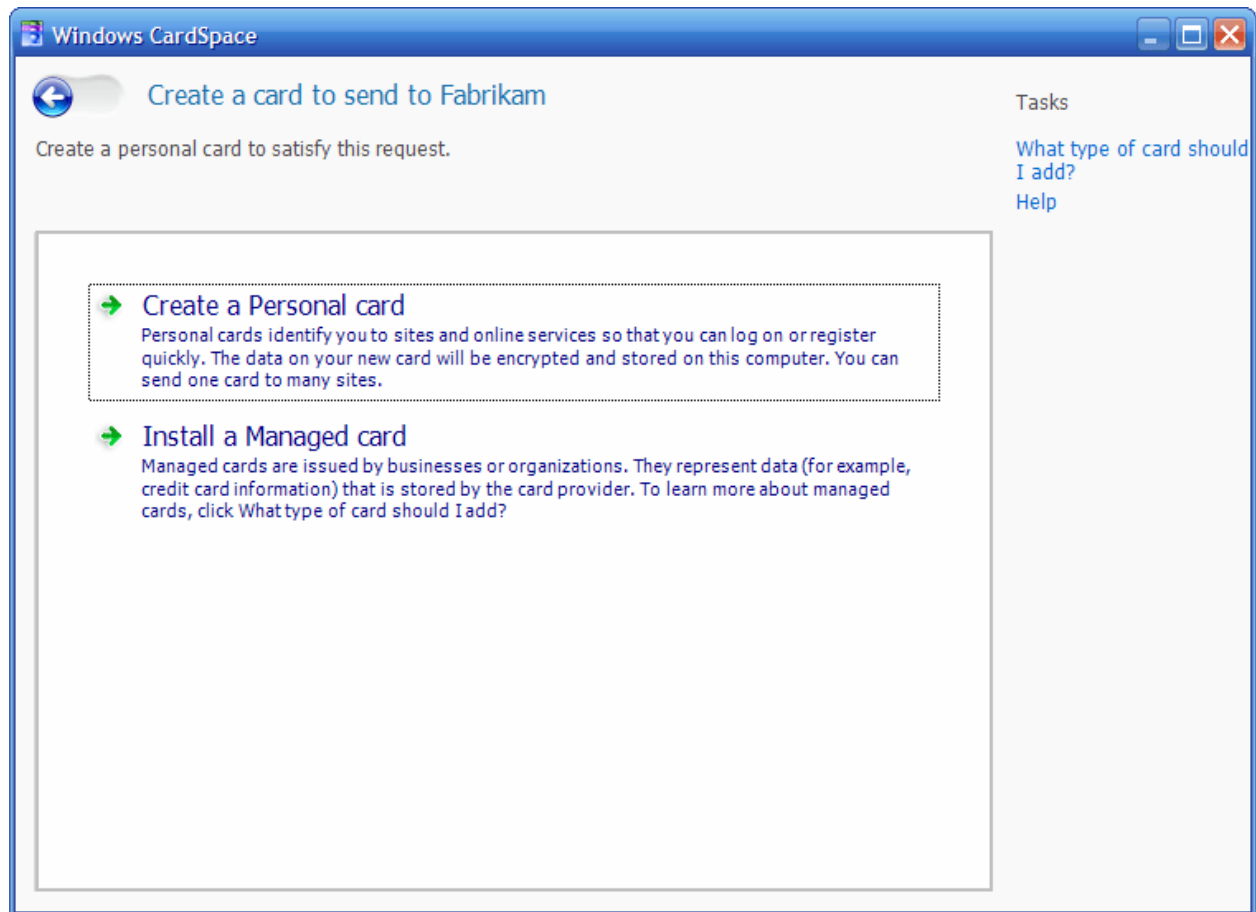
```
<button type="submit">Click here to sign in with your Information Card</button>  
  
<object type="application/x-informationcard" name="xmlToken">  
  
<param name="tokenType" value="urn:oasis:names:tc:SAML:1.0:assertion" />  
  
<param name="issuer" value="http://schemas.xmlsoap.org/ws/2005/05/identity/issuer/self" />  
  
<param name="requiredClaims"  
  value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname  
        http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname  
        http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress  
        http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier" />
```

Cuando se presiona el botón, se muestra el Identity Selector de CardSpace. Esto le permite al usuario seleccionar una identidad de CardSpace.

# Ejemplo



# Ejemplo



# Ejemplo

Windows CardSpace

← Edit a new card

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.

Tasks

[What data should I include on my card?](#)  
[Help](#)

 Personal Card

**Card Properties:**

Card Name:

Image File:

**Card data that will be sent to this site:**

\* First Name:

\* Last Name:

\* Email Address:

**Card data that will not be sent:**

Street:

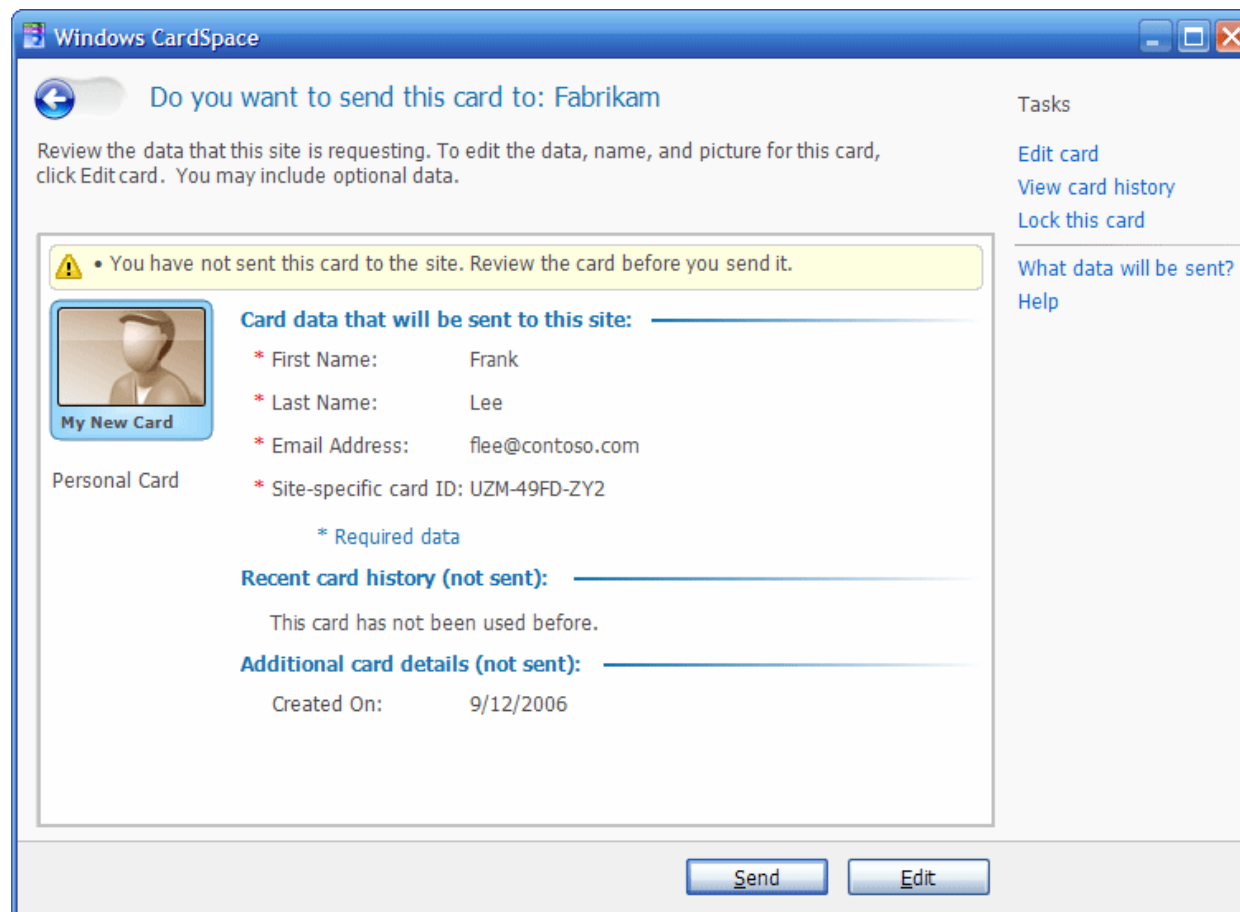
City:

State:

Postal Code:

Country/Region:

# Ejemplo



# Ejemplo

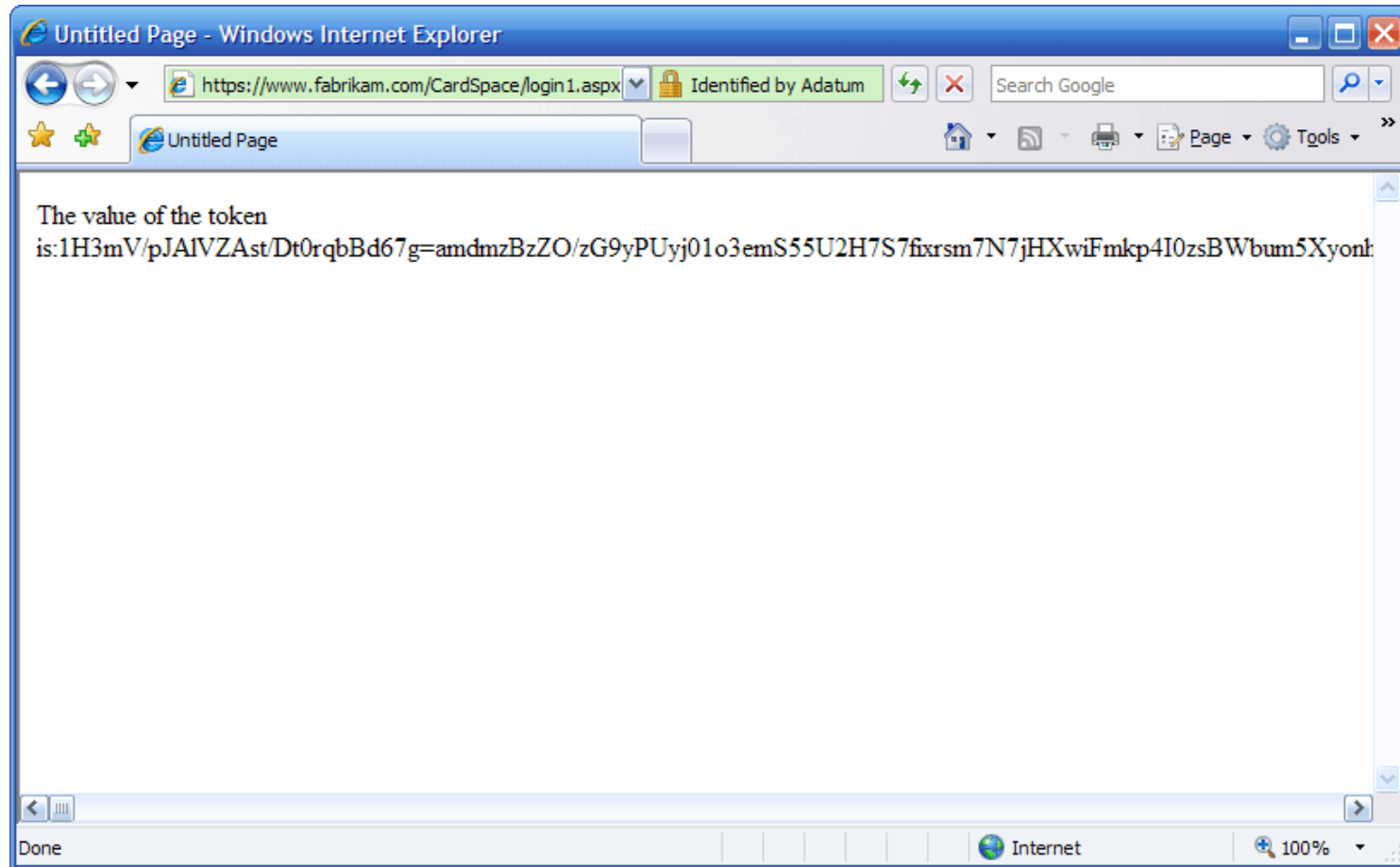
- La información de la tarjeta encriptada es enviada hacia la página **Login1.aspx**.

```
protected void Page_Load(object sender, EventArgs e)
{
    Label1.Text = Request.Params["xmlToken"];
}
```

- Dentro del body de la página HTML.

```
<form id="form1" runat="server">
<div>
The value of the token is:<asp:Label ID="Label1"
runat="server" Text="Label"/>
</div>
</form>
```

# Ejemplo



# Procesar token de información

- Para procesar datos de la información encriptada, los desarrolladores que usan ASP.NET 2.0 pueden utilizar el ejemplo de código **TokenProcessor.cs**.
- La clase **Token** maneja todo el desciframiento y la verificación del token, usando las clases de Windows Communication Foundation.

# Procesar token de información

## **Code Behind**

```
protected void ShowError(string text) {  
    fields.Visible = false;  
    errors.Visible = true;  
    errtext.Text = text;  
}
```

```
protected void Page_Load(object sender, EventArgs e)  
    string xmlToken;  
    xmlToken = Request.Params["xmlToken"];  
    if (xmlToken == null || xmlToken.Equals("")){  
        ShowError("Token presented was null");  
    }  
    else {  
        Token token= new Token(xmlToken);  
        givenname.Text = token.Claims[ClaimTypes.GivenName];  
        surname.Text = token.Claims[ClaimTypes.Surname];  
        email.Text = token.Claims[ClaimTypes.Email]; }  
}
```

# Procesar token de información

- Ésta es la configuración de la información que se tiene que ingresar en el **Web.config** para la clase **Token**.

```
<configuration>
<appSettings>
<add key="MaximumClockSkew" value="60"/>
<add key="CertificateThumbprint"
      value="01234567890ABCDEFEDCBA01234567890ABCDEFEDCBA"/>
<add key="StoreName" value="My"/>
<add key="StoreLocation" value="LocalMachine"/>
<add key="IdentityClaimType"
      value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier"/>
</appSettings>
</configuration>
```

# Procesar token de información

- Cuando el token es descifrado y procesado, podemos ver los valores.

