OpenID en el SIR

Cómo ser un SP sin decírselo a RedIRIS

Miguel Macías Enguídanos
miguel.macias@upv.es

RedIRIS

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

II Foro de Identidad
Cuenca, 06/10/2011

Índice

- OpenID
  - visión general
  - funcionamiento interno
  - las partes buenas
  - intercambio de datos
- SIR
  - soporte OpenID
  - proveedores de servicio (SP)
  - demo
- Taller
  - utilizando OpenID en 3 pasos
  - ¿Y si ya le he dicho a RedIRIS que soy un SP?

¿Qué es OpenID?

- **OpenID** es un mecanismo de autenticación basado en identificadores
  - los identificadores utilizados son URIs o XRIs
- El usuario decide qué identificador va a utilizar para autenticarse en un servicio
- OpenID provee el mecanismo necesario para garantizar que el usuario *controla* dicho identificador
- Las especificaciones OpenID se generan y mantienen desde la *OpenID Foundation* (OIDF):

http://openid.net

Ventajas de OpenID

- El usuario decide quién va a ser su proveedor de identidad, facilitando el SSO
- Evita generar cuentas distintas en cada servicio
  - el usuario tendrá que recordar menos contraseñas
- Las aplicaciones no tienen que implementar la gestión de credenciales
  - almacenamiento de contraseñas, recordatorios, etc.
- Es un mecanismo totalmente descentralizado
  - no se necesita dar de alta ni establecer asociaciones entre el proveedor de identidades y los proveedores de servicios
- Posibilita cualquier tipo de autenticación
  - contraseñas, certificados, biometría, ...

Inconvenientes de OpenID

- Los identificadores de OpenID no son fáciles de recordar (normalmente se utilizan URLs)
  - el término OpenID hace referencia tanto al protocolo como a los identificadores utilizados
- En general, la fiabilidad de los proveedores de identidad no está garantizada
  - ni mucho menos los datos asociados que se puedan obtener en la autenticación
- Hay muchos proveedores de identidad que trabajan con OpenID, pero pocos proveedores de servicios que lo acepten
  - hasta que salgáis de esta charla ;-)

Evolución de OpenID

- 2005
  - protocolo original desarrollado por Brad Fitzpatrick, que estaba trabajando en Six Apart, un proveedor de blogs
- 2006
  - OpenID Authentication 1.1
  - Yadis 1.0 (*Yet another distributed identity system*)
  - OpenID Simple Registration Extension 1.0
- 2007
  - **OpenID Authentication 2.0 (versión actual)**
  - OpenID Attribute Exchange 1.0
- 2008
  - OpenID Provider Authentication Policy Extension 1.0

¿Quién está detrás de OpenID?

Sustaining Corporate Members

Corporate Members

¿Cuál es el futuro de OpenID?

- Actualmente se está trabajando intensamente en la unión de **OpenID** y **oAuth**
- La idea es que OpenID sea el mecanismo básico de autenticación y oAuth el mecanismo de autorización y delegación
- Estado actual:
  - OpenID OAuth Extension (2009)
    http://step2.googlecode.com/svn/spec/openid_oauth_extension/latest/openid_oauth_extension.html
- Futuro (a corto plazo):
  - OpenID Connect
    http://openid.net/connect/

OpenID desde lejos…

- usuario ←→ servicio

  Hola, soy http://mi.url.de.open.id →

  ← Mmmmm… no me lo creo. Que me lo diga tu servidor

- usuario ←→ servidor

  Hola, quiero demostrarle al servicio quién soy →

  ← Demuéstramelo a mí primero y ya veremos

  …

  ← Vale, dile al servicio que ya lo he comprobado

- usuario ←→ servicio

  Listo, que dice el servidor que es verdad →

  ← Espera un momento

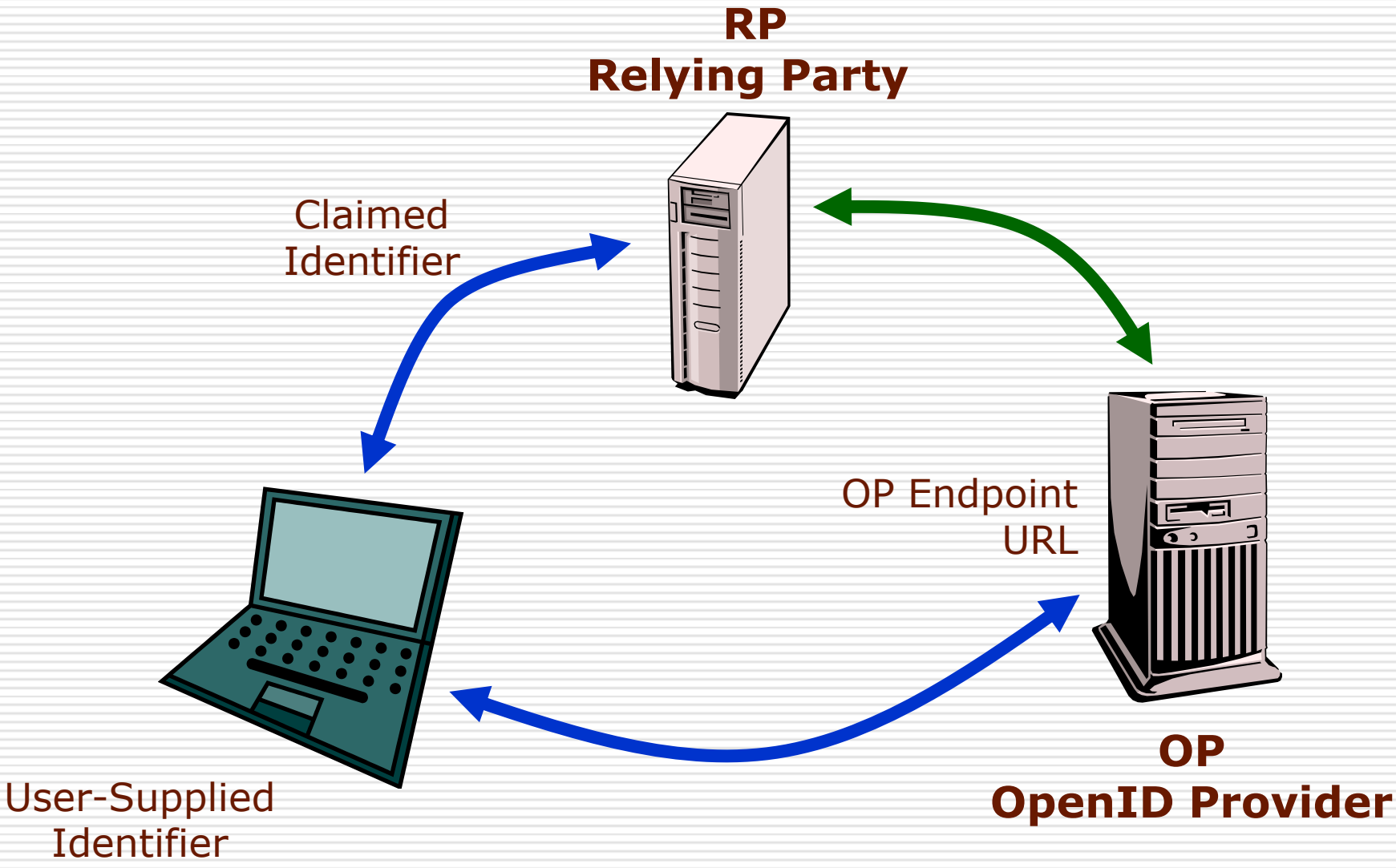
- servicio ←→ servidor

  ¿Es verdad lo que dice éste? →

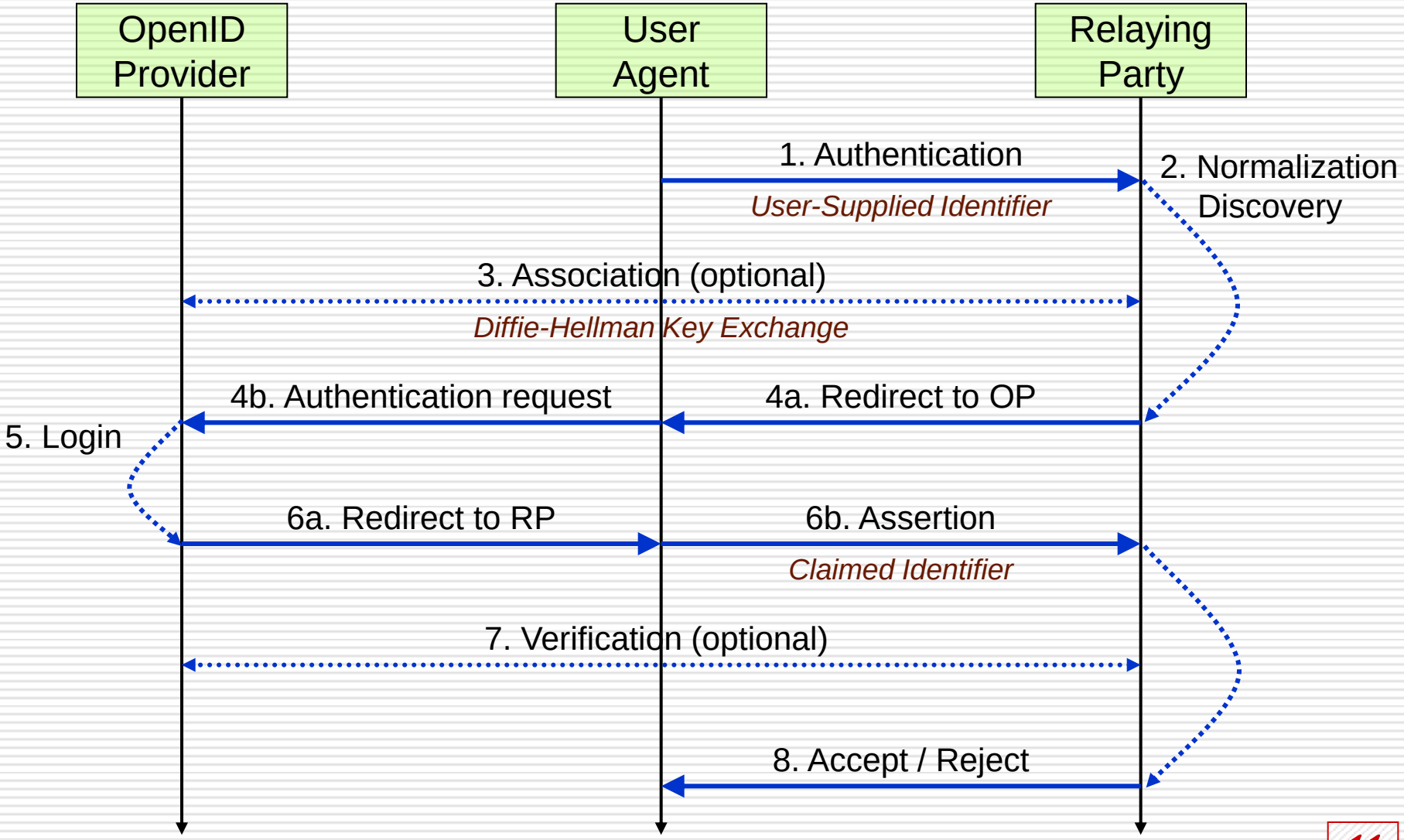
  ← Sí, lo he comprobado

← **¡Adelante!**

Nomenclatura OpenID



OpenID desde cerca…



OpenID: reputación

- El protocolo OpenID ha tenido muchas críticas en cuanto a la seguridad y efectividad del mecanismo
  - **algunas** de ellas hay que tenerlas en cuenta
- Tras un auge, a partir de la versión 2.0, en la que aparecieron multitud de OPs…
- … vino un paréntesis en el uso de OpenID
- Hasta la aparición de las redes sociales y sus necesidades de autenticación
  - Facebook y Google apuestan abiertamente por OpenID
- Aunque, quizás, el factor más importante para la reputación de OpenID haya pasado desapercibido por aquí…

OpenID en la administración USA

- La administración de Estados Unidos acepta (y promueve) el uso de OpenID como mecanismo de autenticación para sus webs oficiales
  - desde finales de 2009 y para el nivel 1 de seguridad (transacciones de bajo riesgo)
- Hace un uso 'moderno' de OpenID
  - eliminando las *concesiones* del estándar y estableciendo medidas de seguridad adicionales
- Los OP que quieran participar en este proyecto tienen que certificarse
  - actualmente: Google, PayPal, VeriSign y Wave Systems http://openidentityexchange.org/certified-providers

Entonces ¿usamos OpenID?

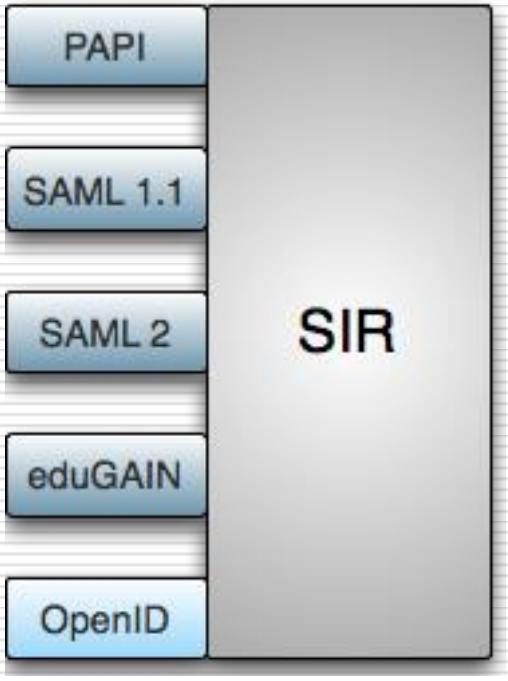
- OpenID es un mecanismo de autenticación seguro y robusto si se usa 'correctamente':
  - sólo confiamos en determinados OP
  - el usuario no tiene que recordar su OpenID ni tiene que suministrarlo, sólo elegir un OP de los que le presentamos
  - todas las comunicaciones se establecen con HTTPS
  - todos los certificados digitales se comprueban y se validan sobre las entidades raíz en las que confiemos
  - El RP proporciona la política de uso de los datos obtenidos a través de OpenID
  - El OP solicita el consentimiento antes de permitir la autenticación/autorización del usuario
  - El RP también permite su descubrimiento por parte del OP

OpenID: intercambio de datos

- Además de la autenticación, OpenID también puede utilizarse para el intercambio de datos
- **SReg** (**S**imple **Reg**istration Extension)
  - extensión que permite suministrar los datos básicos necesarios para registrar una cuenta en un servicio:
    - nombre completo, alias, email, sexo, fecha de nacimiento, idioma, código postal, país y zona horaria
- **AX** (**A**ttribute E**x**change)
  - es una extensión a OpenID que permite el intercambio de datos entre el RP y el OP
    - los datos a intercambiar y el tipo de los mismos se definen en base a esquemas
    - ej.: http://schema.openid.net/contact/email

Servicio de Identidad de RedIRIS

- El SIR soporta OpenID como protocolo de salida
  - ➔ toda institución federada a través del SIR es un OpenID Provider
- Los identificadores OpenID son URLs en cualquier lengua oficial:
  - https://yo.rediris.es/soy/usu@institu.cion/
  - https://eu.rediris.es/son/usu@institu.cion/
  - https://jo.rediris.es/soc/usu@institu.cion/
  - https://ni.rediris.es/usu@institu.cion/naiz/



- Se permite (en algunos sitios) que el usuario utilice un identificador corto para iniciar la autenticación
  - https://yo.rediris.es/

SIR: personalización OpenID

- Para generar el identificador OpenID (la parte personal) se utiliza el siguiente orden:
  - uid@sHO (*userid + schacHomeOrganization*)
  - cn@sHO (*commonName+ sHO*)
  - ePTI@sHO (*eduPersonTargetedID + sHO*)
  - iMMA (*irisMailMainAddress*)
- Además, para las aplicaciones registradas, se utiliza la extensión SReg para proporcionar los datos:
  - email
  - fullname
  - nickname

    siempre que la institución los entregue y el usuario consienta

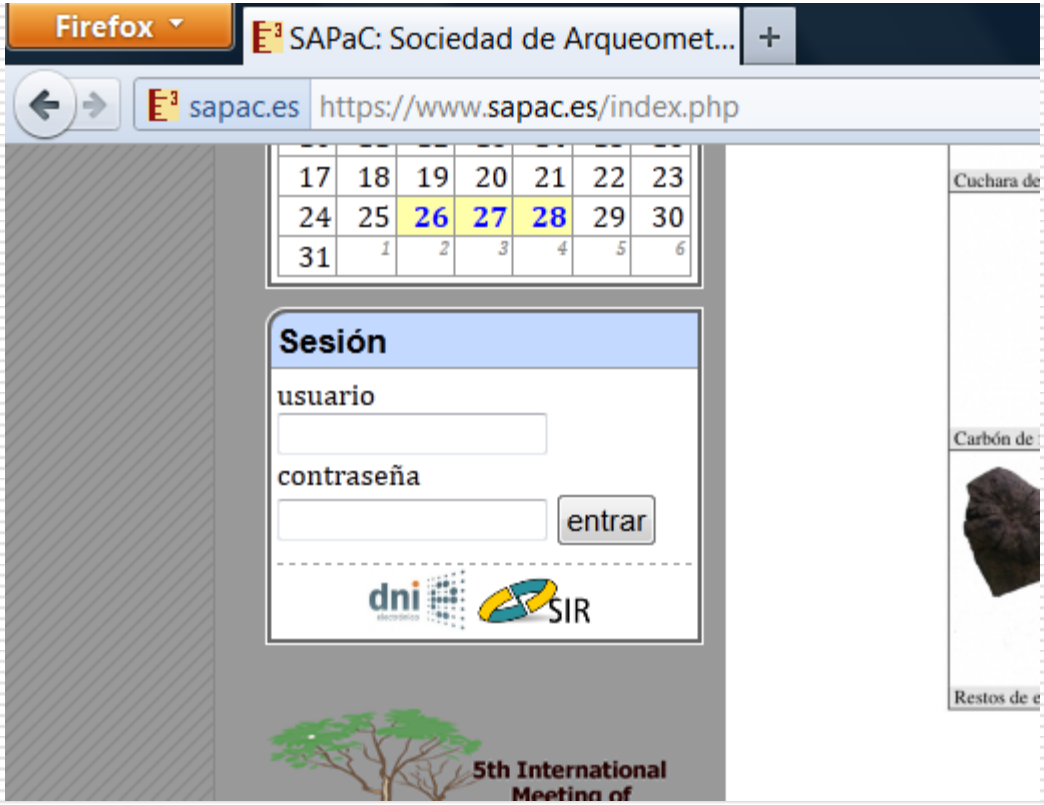
SIR: proveedores de servicio

http://www.rediris.es/sir/docs/howto-sp.html

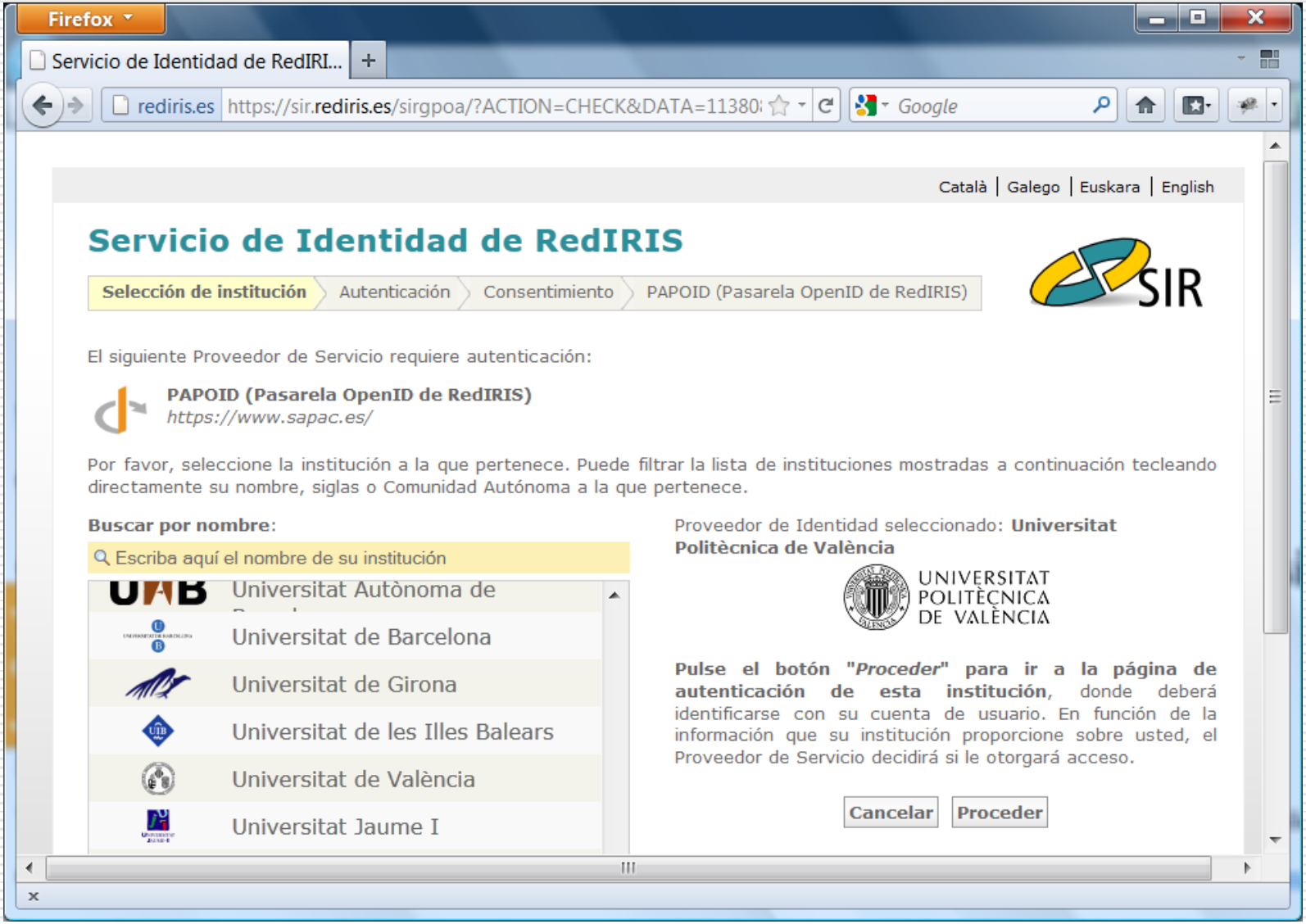
- Para participar como SP en el SIR es necesario:
  - Desplegar un SP de alguno de los protocolos soportados…
  - Contactar con los responsables técnicos del SIR…
  - …hacer llegar a RedIRIS el documento de Condiciones de Uso del SIR para SPs… validado por el PER…
  - Actualizar el SP con los metadatos…
  - El equipo técnico del SIR procederá a la instalación del nuevo SP…
- Con OpenID… **no es necesario nada de esto**
  - bueno, desplegar un SP que sepa hablar OpenID sí
  - y si no decimos nada… ¡no tendremos datos de SReg!

Demo: SAPaC

- Esta aplicación soporta varios mecanismos de autenticación:
  - usuarios locales
  - DNI electrónico
  - SIR (con OpenID)

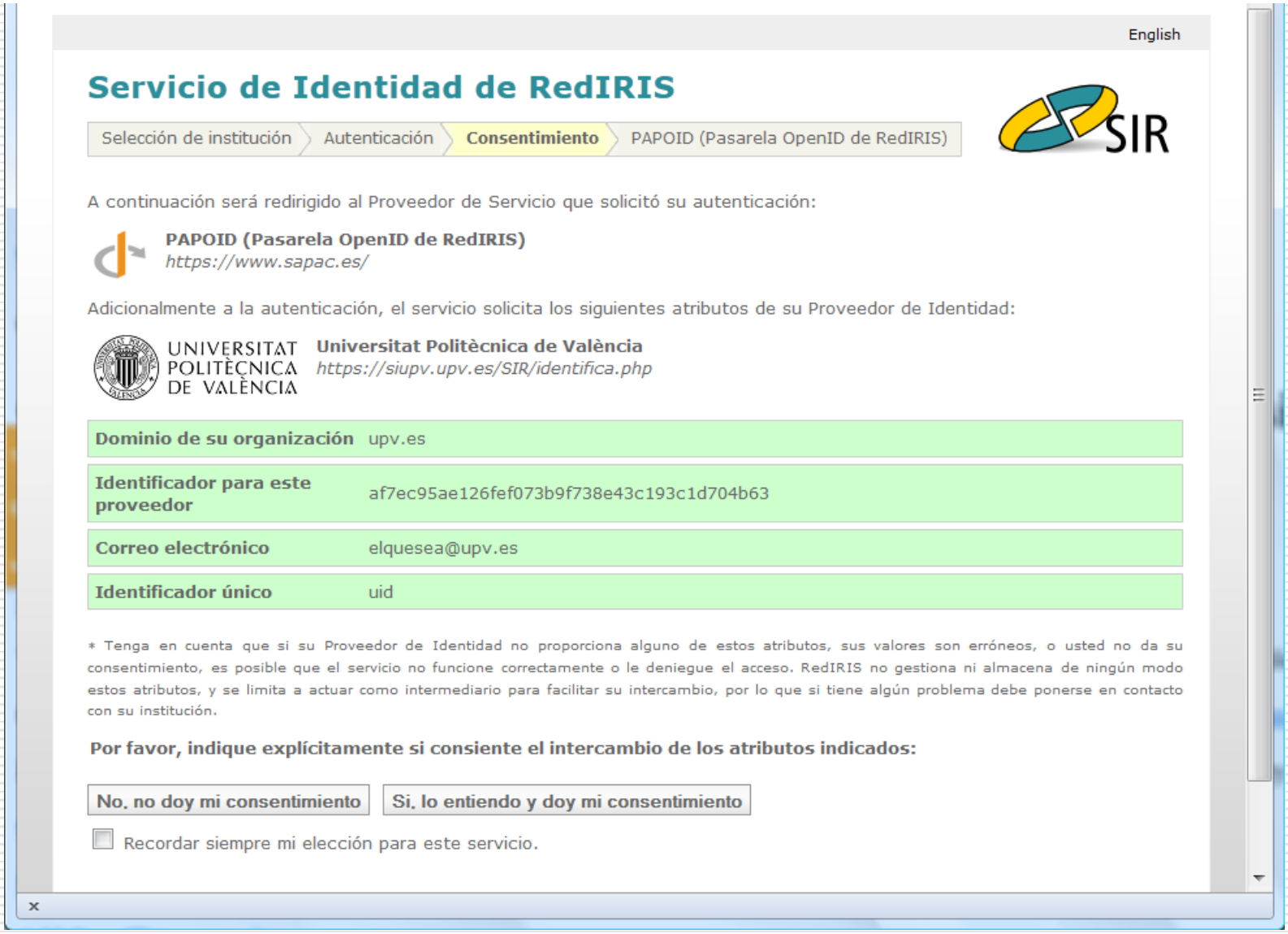


Demo: WAYF


Firefox
Servicio de Identidad de RedIRI...
rediris.es
https://sir.rediris.es/sirgpoa/?ACTION=CHECK&DATA=11380
Google
Català | Galego | Euskara | English
Servicio de Identidad de RedIRIS
Selección de institución
Autenticación
Consentimiento
PAPOID (Pasarela OpenID de RedIRIS)
SIR
El siguiente Proveedor de Servicio requiere autenticación:
PAPOID (Pasarela OpenID de RedIRIS)
https://www.sapac.es/
Por favor, seleccione la institución a la que pertenece. Puede filtrar la lista de instituciones mostradas a continuación tecleando directamente su nombre, siglas o Comunidad Autónoma a la que pertenece.
Buscar por nombre:
Escriba aquí el nombre de su institución
Universitat Autònoma de
Universitat de Barcelona
Universitat de Girona
Universitat de les Illes Balears
Universitat de València
Universitat Jaume I
Proveedor de Identidad seleccionado: Universitat Politècnica de València
UNIVERSITAT POLITÈCNICA DE VALÈNCIA
Pulse el botón "Proceder" para ir a la página de autenticación de esta institución, donde deberá identificarse con su cuenta de usuario. En función de la información que su institución proporcione sobre usted, el Proveedor de Servicio decidirá si le otorgará acceso.
Cancelar
Proceder

Demo: Autenticación local

Demo: Consentimiento



Taller: utilizando OpenID

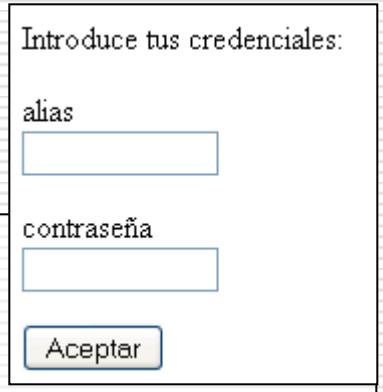
- Para utilizar OpenID desde nuestras aplicaciones es conveniente utilizar alguna de las librerías ya existentes:

  http://openid.net/developers/libraries/

- En este taller vamos a ver cómo utilizar OpenID desde una aplicación en **PHP** utilizando la librería **LightOpenID**:
  - http://gitorious.org/lightopenid#more
- Requisitos:
  - PHP >= 5
  - CURL (recomendado) o PHP streams
  - LightOpenID

Taller: Formulario de autenticación

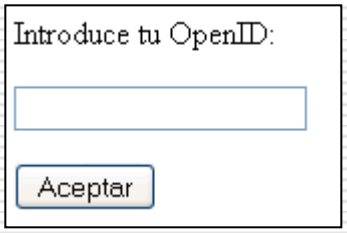
- Partimos de una aplicación que tiene el típico formulario de autenticación con cuentas locales




```
<form method="post" action="">
  <p>Introduce tus credenciales:</p>
  <p><label for="alias">alias</label><br />
    <input name="alias" type="text"
          id="alias" size="12" maxlength="14" /></p>
  <p><label for="password">contrase&ntilde;a</label><br />
    <input name="password" type="password"
          id="password" size="12" maxlength="60" /></p>
  <p><input type="submit" value="Aceptar" /></p>
</form>
```

Taller: introduciendo OpenID

- Sustituimos la auntenticación con cuentas locales por autenticación OpenID




```
<form method="post" action="">
  <p>Introduce tu OpenID:</p>
  <p><input name="openid_identifier" type="text"
            size="20" maxlength="1024" /></p>
  <p><input type="submit" value="Aceptar" /></p>
</form>
```

- Pero esta no es la mejor opción
  - ¿aceptamos cualquier OP?
  - ¿le pedimos al usuario que recuerde su OpenID?

Taller: al SIR por OpenID

- Le indicamos al usuario que puede entrar a nuestra aplicación desde el SIR
  - el usuario no tiene que saber nada acerca de OpenID


```
<form method="post" action="">
  <p>Autent&iacute;cate a trav&eacute;s del SIR:</p>
  <p><input type="image" src="sir.png"
                    alt="Servicio de Identidad de RedIRIS"
            name="SIR" /></p>
</form>
```

- Podríamos añadir tantos OP como quisiéramos

Taller: implementando el protocolo 1/3

```php
// cargamos la librería LightOpenID
require 'openid.php';

// instanciamos el objeto que implementa OpenID
$openid = new LightOpenID($_SERVER['SERVER_NAME']);

// establecemos que queremos validar los certificados
$openid->verify_peer= true;
$openid->cainfo= pathinfo($_SERVER['SCRIPT_FILENAME'],
                          PATHINFO_DIRNAME) .
                 DIRECTORY_SEPARATOR .
                 'ca-bundle.pem';
```

(sigue)

- El fichero **`ca-bundle.pem`** contiene los certificados de las entidades raíz en las que confiamos
  - es un fichero de texto donde se van concatenando todos los certificados en formato PEM
- El RP se conectará al OP utilizando HTTPS

Taller: implementando el protocolo 2/3

```php
// comprobamos en qué fase de la autenticación estamos
if(!$openid->mode) {
    // el usuario se quiere autenticar
    // -> nosotros establecemos su OpenID
    $openid->identity = 'https://yo.rediris.es/';    // OpenID del SIR

    // indicamos qué atributos queremos leer
    $openid->required = array('namePerson/friendly', 'contact/email');
    $openid->optional = array('namePerson/first');

    // y lanzamos el mecanismo de autenticación
    header('Location: ' . $openid->authUrl());

} elseif($openid->mode == 'cancel') {
    // el usuario ha cancelado la autenticación
    . . .
} else {
    // el proceso ha terminado
                    (este bloque de código está en la siguiente página)
}
```

- A esta página se entra varias veces

Taller: implementando el protocolo 3/3

```
// comprobamos en qué fase de la autenticación estamos
if(!$openid->mode) {
    . . .
} elseif($openid->mode == 'cancel') {
    . . .
} else {
    // se ha terminado el proceso
    if ($openid->validate()) {
        // la validación es correcta
        $idOpenID= $openid->identity;
        // comprobamos el OpenID y extraemos información del mismo
        if (preg_match('#^https://yo\.rediris\.es/soy/' .
                                '((.+)@(\w+\.)+[a-z]{2,4})/?$#',
                        $idOpenID, $usrOpenID)) {
            $listaAtributos= $openid->getAttributes();
           . . .
        }
    }
    else {
        // la validación no es correcta
        . . .
    }
}
```

Taller: identificadores OpenID

- Proporcionar automáticamente el identificador inicial del usuario tiene varias ventajas:
  - no hay que explicarle al usuario qué es OpenID
  - podemos utilizar un identificador con HTTPS desde el principio (evita posibles ataques de *Man in the Middle*)
- Si nuestra aplicación acepta usuarios de cualquier institución de RedIRIS:
  - https://yo.rediris.es/
- Si queremos aceptar sólo usuarios de nuestra institución (evitando el WAYF):
  - https://yo.rediris.es/soy/@institu.cion
  - con el logo de nuestra institución en lugar del SIR

Taller: resumen

- Implementar OpenID en una aplicación es sencillo
- No se necesita ningún paso previo (ni CUSO, ni claves, …) para utilizar OpenID
- Con el mismo código podemos aceptar usuarios de nuestra institución y/o usuarios de RedIRIS


- No tenemos datos (email, rol, etc.) de los usuarios autenticados
  - hay que buscar alternativas si se necesitan para la autorización o decirle a RedIRIS que somos un SP (si nos basta con el email)
- Nos hemos creado una dependencia con RedIRIS

Taller: a tener en cuenta

- El identificador de OpenID pasa a ser la clave con la que reconocemos a los usuarios
  - si eres un OP → no reutilices identificadores
  - si eres un RP → permite al usuario asociar varios OpenID
- Si ya tienes usuarios locales, puedes permitir que los usuarios asocien sus OpenID a sus cuentas
- Si vas a dar de alta a nuevos usuarios a partir de su identificador OpenID:
  - solicita los datos (nombre, email) que necesites para el registro (aunque estés preparado para no recibirlos)
  - una opción adecuada en algunas ocasiones es dar de alta a usuarios pre-cargados (con su email, por ejemplo)

¡Ya soy un SP en el SIR!

- Si te interesa OpenID y ya tienes en marcha el **phpPoA**, ahora puedes utilizar OpenID como método de autenticación

  http://forja.rediris.es/projects/phppoa/

- Puedes configurar en qué OPs confías y cómo extraer datos a partir del identificador OpenID
- La página de entrada es personalizable, pudiendo generar la interfaz de usuario que desees
- Se puede establecer que el mecanismo de autenticación se lance automáticamente

OpenID en el SIR

GRACIAS POR TU ATENCIÓN

Como ser un SP sin decírselo a RedIRIS

Miguel Macías Enguídanos
miguel.macias@upv.es

RedIRIS

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

II Foro de Identidad
Cuenca, 06/10/2011