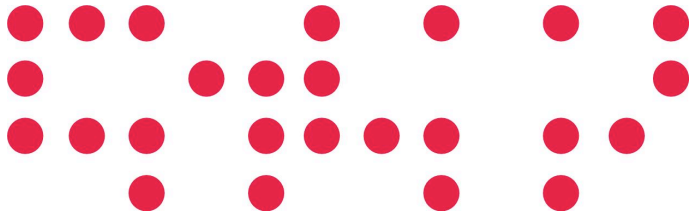
Servicio de Identidad de RedIRIS

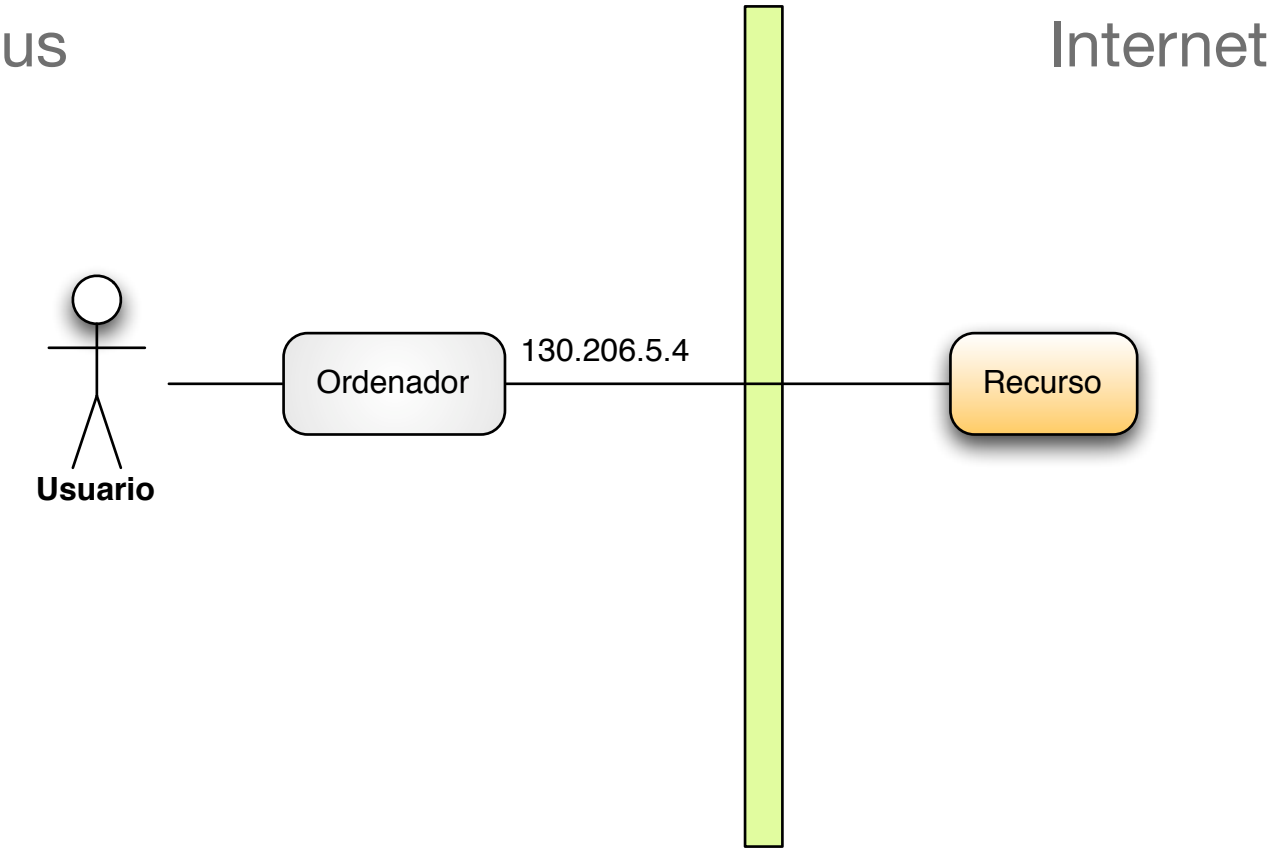
Acceso federado a e-recursos

Cándido Rodríguez
candido.rodriguez@rediris.es

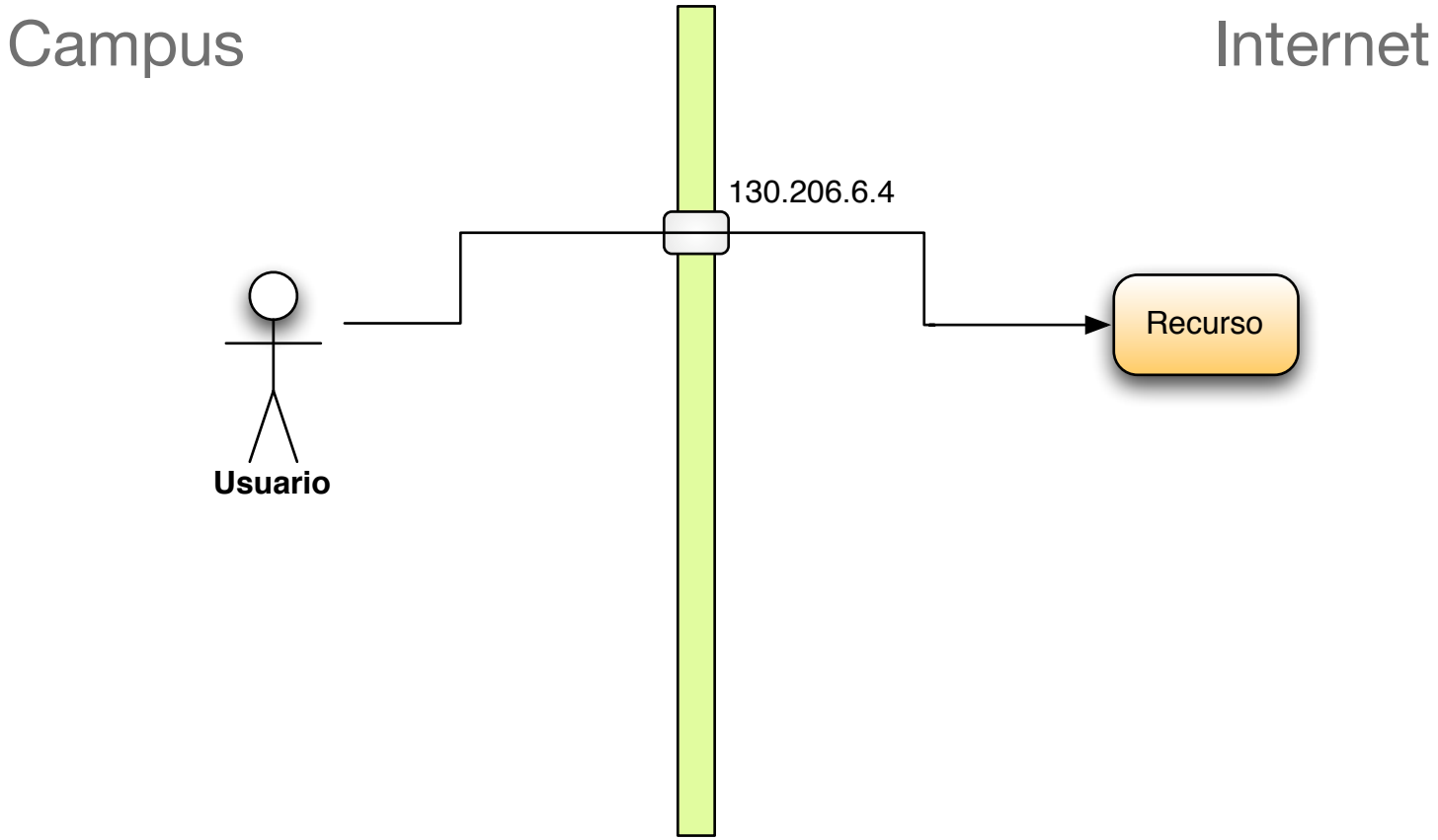
1. **Hacia las federaciones**
2. **Servicio de Identidad de RedIRIS (SIR)**
3. **Arquitectura de SIR**
4. **Estadísticas**
5. **Futuro**
6. **¿Cómo unirse?**



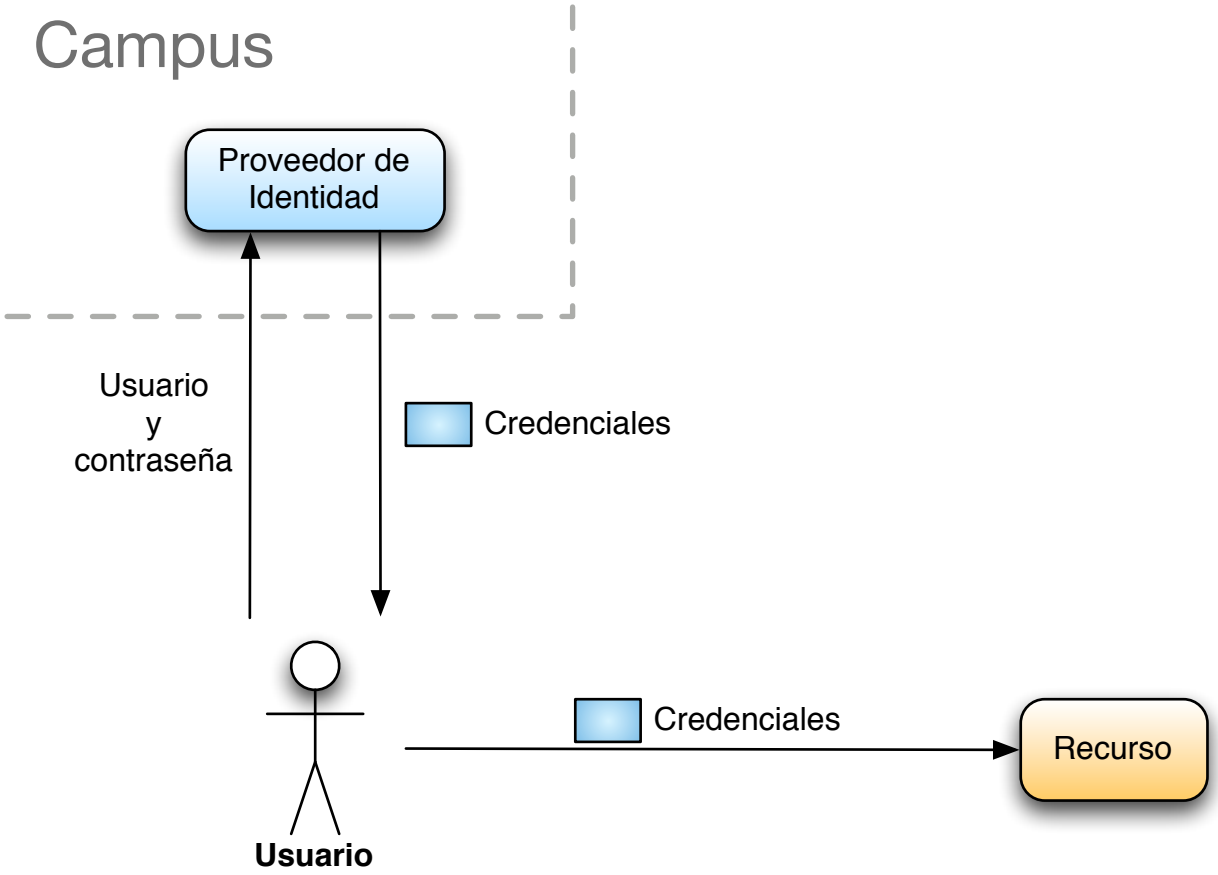
- Control por IP



- Acceso a través de Proxy/VPN



- Acceso a través de una federación



Hacia las federaciones

- Una federación es un esquema de confianza que permite la colaboración entre sus participantes
  - Mediante el intercambio de datos
  - En nuestro caso, datos sobre la identidad de los usuarios
    - Personas y aplicaciones
- Los proveedores de identidad (IdP) establecen identidades y distribuyen datos relativos a ellas
  - Dentro del entorno local
  - Bajo control del usuario
- Los proveedores de servicio (SP) usan estos datos y los usan para decidir los derechos de acceso y personalizar las aplicaciones
  - Aplicando sus propias políticas

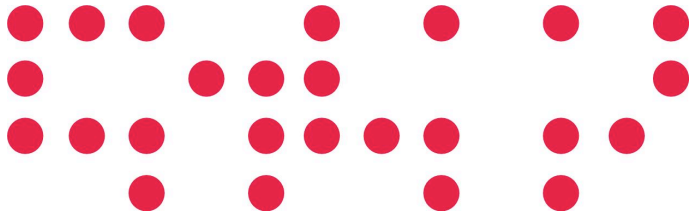
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Ventajas de una federación
  - No se gestionan las cuentas de usuario de instituciones externas
    - Reducimos costes en la gestión de nuestra infraestructura
    - Baja la complejidad de las políticas de seguridad
    - Cumplimos con la LOPD
  - Los usuarios sólo tienen que recordar un par usuario/contraseña
    - Menos post-it ➔ más seguridad
  - El usuario no tiene que solicitar uno a uno acceso a los proveedores de servicio
    - Una vez que añadimos un recurso a la federación, queda potencialmente disponible para el usuario

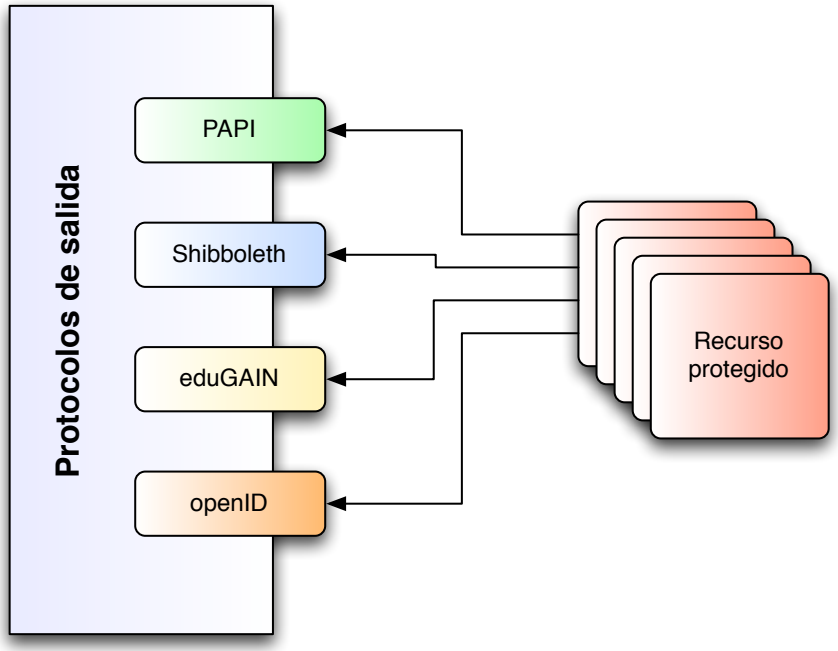
Agenda

1. **Hacia las federaciones**
2. **Servicio de Identidad de RedIRIS (SIR)**
3. **Arquitectura de SIR**
4. **Estadísticas**
5. **Futuro**
6. **¿Cómo unirse?**

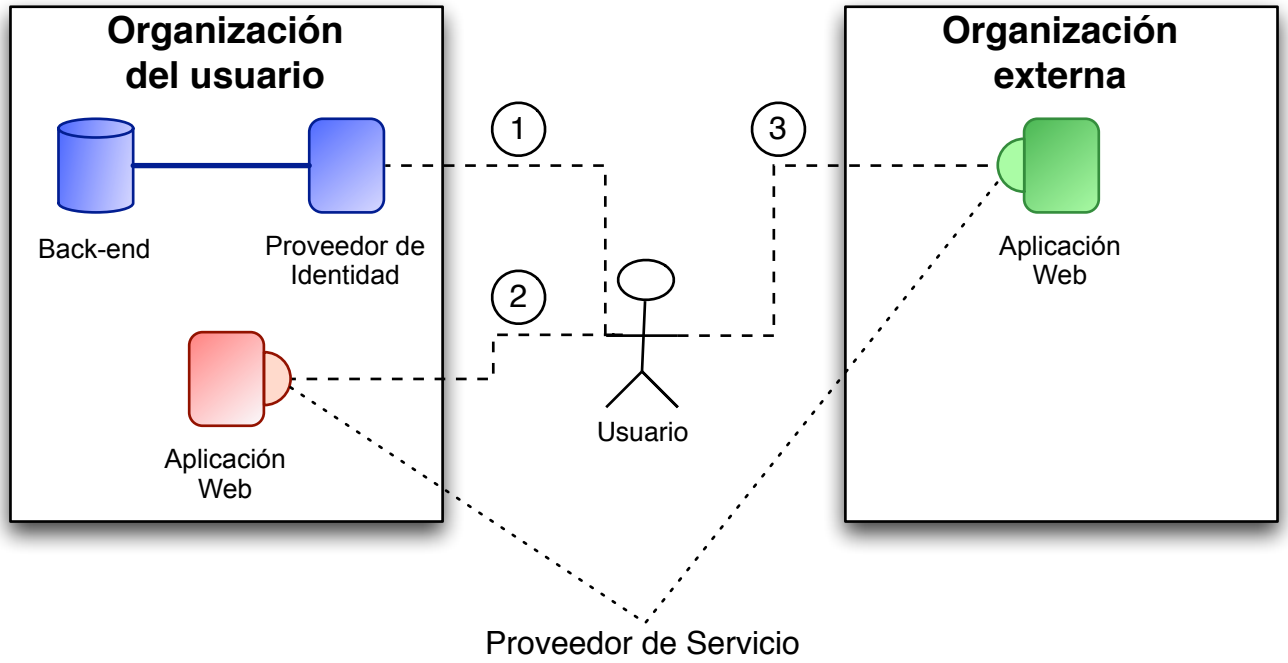


- Es un hub de interconexión entre proveedores de identidad y de servicio
  - Instituciones dando acceso a sus usuarios
  - Recursos protegidos potencialmente disponibles a todas las instituciones
- Bases de una federación
  - Proveedor de identidad
    - Realiza la autenticación del usuario y emite los atributos del usuario
  - Proveedor de servicio
    - Comprueba las credenciales del usuario para realizar la autorización en el acceso al servicio
- Papel de RedIRIS en esta federación
  - Actúa de intermediaro de confianza

- La federación SIR soporta los siguientes protocolos:
  - PAPI v1
  - SAML 1.1 (Shibboleth 1.3) y SAML 2 (Shibboleth 2)
  - eduGAIN con perfil SAML 1.1
  - OpenID 1 y 2

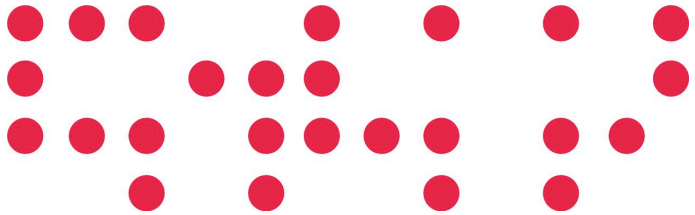


- El funcionamiento del SIR se basa en tecnologías de federación de identidades



Agenda

1. **Hacia las federaciones**
2. **Servicio de Identidad de RedIRIS (SIR)**
3. **Arquitectura de SIR**
4. **Estadísticas**
5. **Futuro**
6. **¿Cómo unirse?**

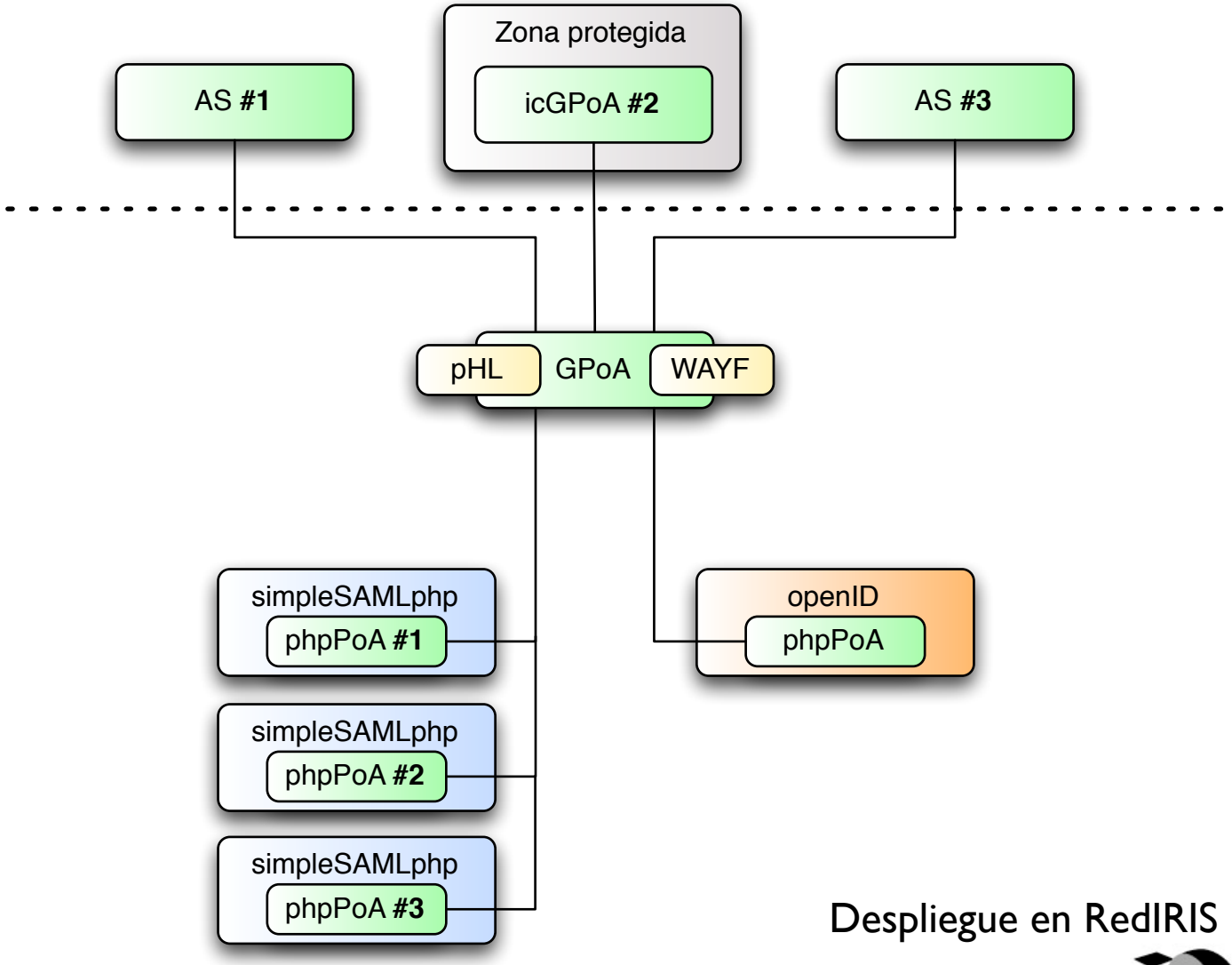


- Dos federaciones desplegadas
  - SIRtest: federación de prueba
    - Se valida previamente la infraestructura técnica de proveedores de identidad y de servicio
      - PAPI
      - SAML 1.1/2
      - OpenID
    - No hay que firmar ningún documento para solicitar su uso
  - SIR: federación en producción
    - Una vez queda valido, hay que firmar el documento de condiciones de uso

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

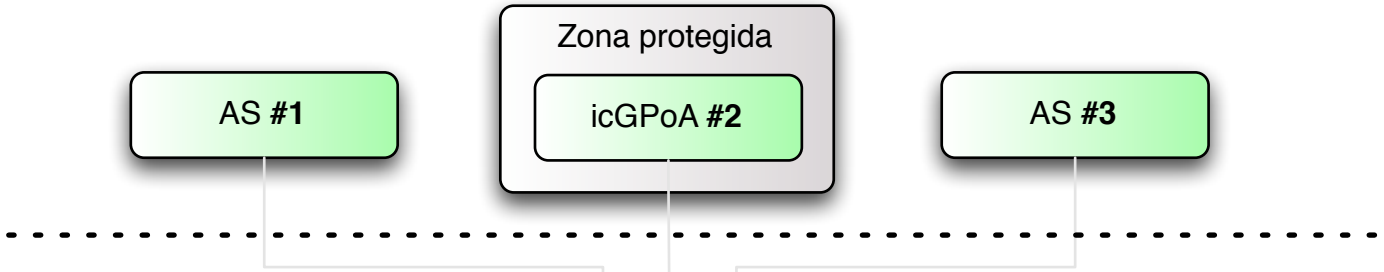
Despliegue en la institución



Despliegue en RedIRIS

Red IRIS

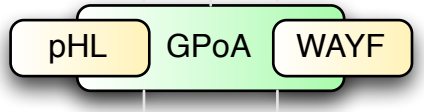
Despliegue en la institución



- Proveedor de identidad
  - Basado en tecnología PAPI
    - AuthServer (AS)
    - icGPoA
      - ¡Si puedes protegerlo, tienes un AS!
  - Debe incorporar la clave pública del GPoA del SIR
    - Metadatos para PAPI disponibles

Despliegue en la institución

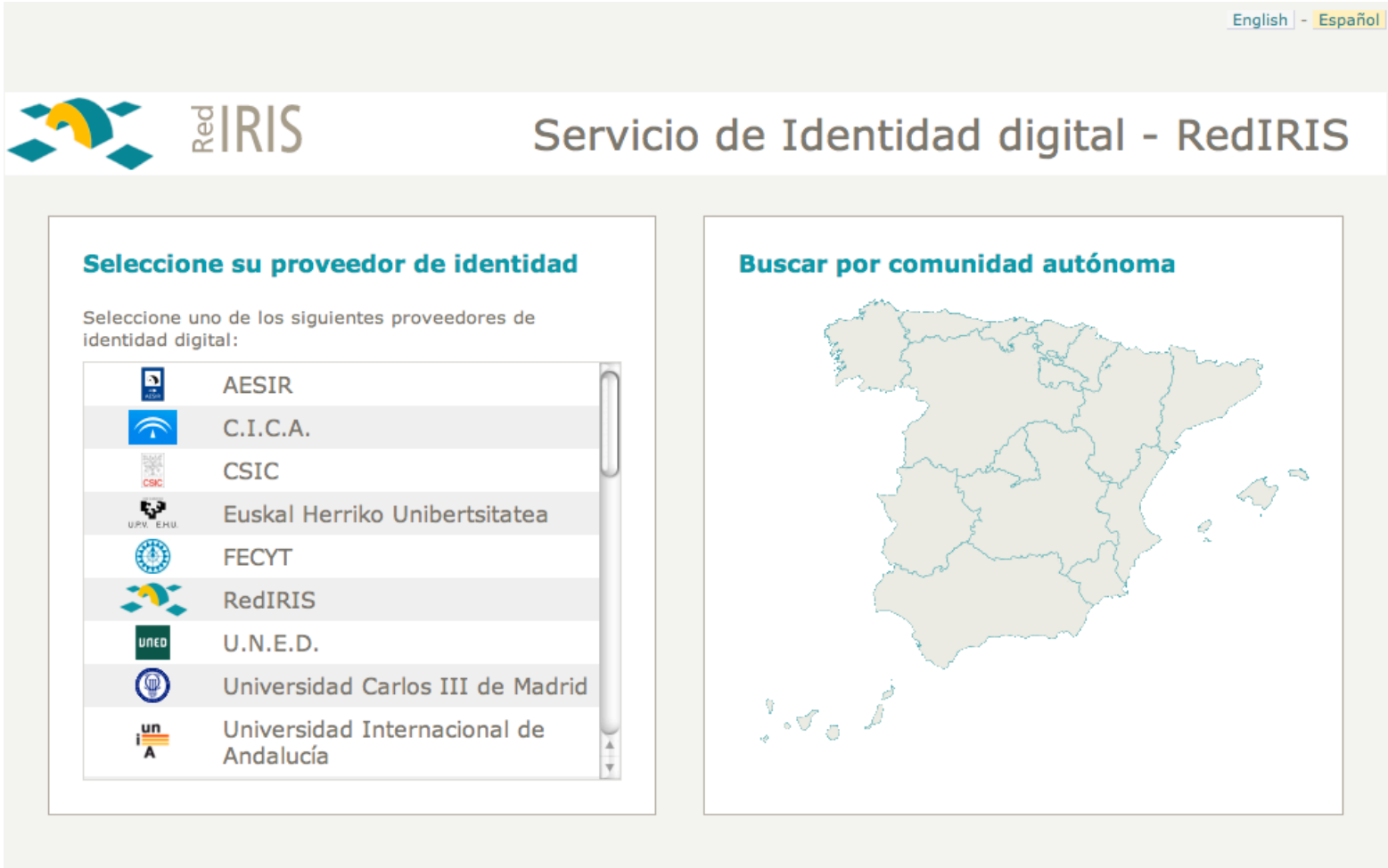
- GPoA de SIR
  - Es el motor de la federación



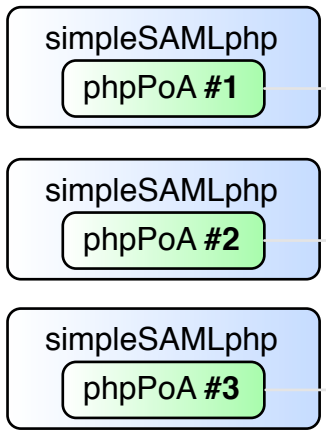
  - Incorpora dos componentes principales
    - Where Are Your From? (WAYF)
      - Pregunta al usuario cuál es su institución
    - PAPI Home Locator (pHL)
      - Indica al GPoA cuál es la institución del usuario

Despliegue en RedIRIS

- Where Are Your From? (WAYF)

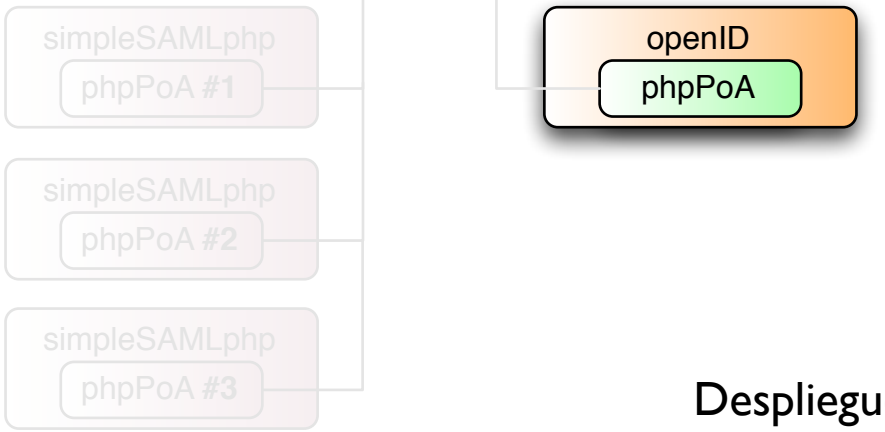


- SAML 1.1 y SAML 2 en SIR
  - Por cada proveedor de identidad se despliega simpleSAMLphp
    - Es protegido por un phpPoA que especifica su AS a través del pHL
  - RedIRIS publica los metadatos con los interfaces de salida para SAML 1.1
  - Si la institución tiene ya una solución para SAML 1.1
    - En vez de desplegar simpleSAMLphp, podemos incluir sus metadatos



Despliegue en la institución

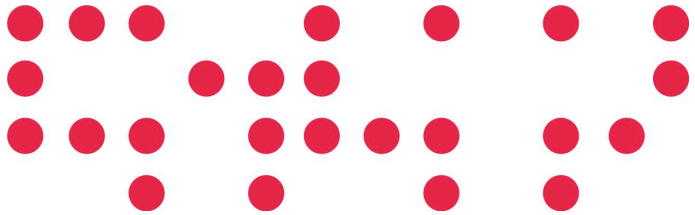
- OpenID en SIR
  - Toda institución en SIR ofrece identidad OpenID a sus usuarios
    - Condición: emitir atributo UID
  - Usuario:
    - http://yo.rediris.es/soy/kan@rediris.es
    - http://eu.rediris.es/son/kan@rediris.es
    - http://jo.rediris.es/soc/kan@rediris.es
    - http://ni.rediris.es/kan@rediris.es/naiz



Despliegue en RedIRIS

Agenda

1. **Hacia las federaciones**
2. **Servicio de Identidad de RedIRIS (SIR)**
3. **Arquitectura de SIR**
4. **Estadísticas**
5. **Futuro**
6. **¿Cómo unirse?**



Estadísticas

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Proveedores de identidad

28 instituciones

- AESIR
- C.I.C.A.
- CSIC
- Euskal Herriko Unibertsitatea
- FECYT
- RedIRIS
- U.N.E.D.
- Universidad Carlos III de Madrid
- Universidad Internacional de Andalucía
- Universidad Pablo de Olavide
- Universidad Rey Juan Carlos
- Universidad de Alcalá de Henares
- Universidad de Burgos
- Universidad de Cádiz
- Universidad de Córdoba
- Universidad de Extremadura

- Universidad de Burgos
- Universidad de Cádiz
- Universidad de Córdoba
- Universidad de Extremadura
- Universidad de La Rioja
- Universidad de León
- Universidad de Málaga
- Universidad de Salamanca
- Universidad de Sevilla
- Universidade de Santiago de Compostela
- Universidade de Vigo
- Universitat Jaume I
- Universitat Oberta de Catalunya
- Universitat Politècnica de Catalunya
- Universitat Rovira i Virgili
- Universitat de València
- Universitat de les Illes Balears

Estadísticas

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Proveedores de servicio

MetaPress

Microsoft DreamSpark™
DREAM TODAY. CREATE TOMORROW

SCOPUS

ScienceDirect

PATHOLOGY IMAGES
Collection of high resolution histological pictures

ISI Web of Knowledge℠

IOP Institute of Physics

SpringerLink

OpenID

universia
red de universidades, red de oportunidades

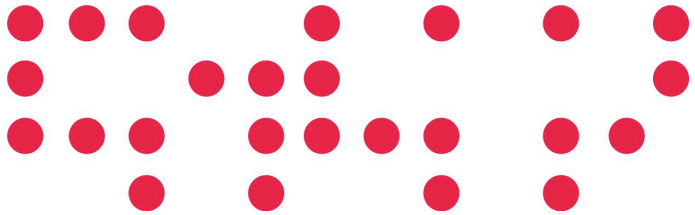
DOPPLR

LIVEJOURNAL™

RedIRIS

Agenda

1. **Hacia las federaciones**
2. **Servicio de Identidad de RedIRIS (SIR)**
3. **Arquitectura de SIR**
4. **Estadísticas**
5. **Futuro**
6. **¿Cómo unirse?**

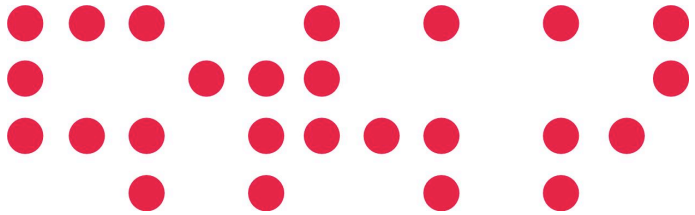


Futuro

- URLs de acceso directo al proveedor de servicio
- Evolucionar hacia modelo *user-centric*
  - Consentimiento de atributos por parte del usuario
    - Firmar con su certificado digital los atributos
  - yo.estoy
    - Portal 2.0 para el usuario final
    - Gestión de los atributos
    - Lista de proveedores de servicio disponibles
      - Gestión de *bookmark*
- Level of Assurance (LoA)
  - Nivel de confianza según método de autenticación
- Experimientar con nuevas tecnologías
  - Piloto de InfoCard de Microsoft

Agenda

1. **Hacia las federaciones**
2. **Servicio de Identidad de RedIRIS (SIR)**
3. **Arquitectura de SIR**
4. **Estadísticas**
5. **Futuro**
6. **¿Cómo unirse?**



¿Cómo unirse?

- Como proveedor de identidad
  - Desplegar un AS o un icGPoA
  - Solicitar su inclusión en SIRtest
  - Realizar pruebas técnicas
    - PAPI
    - SAML 1.1
    - OpenID
  - Firmar documento de condiciones de uso
  - Por cada recurso protegido que utilice, si dispone de tecnología para conectarse a una federación
    - Ponerlos en contacto con el equipo técnico del SIR
    - Se integra así con el sistema de SSO de la institución

¿Cómo unirse?

- Como proveedor de servicio
  - Solicitar su inclusión en SIRtest
    - Indicar qué tecnología utiliza para federarse
    - Indicar qué atributos requiere
  - Realizar pruebas técnicas
  - Firmar documento de condiciones de uso

"Creo que jamás montaré una cosa de la que tenga menos idea que esto del sir. Instalación, mantenimiento y uso, cero pelotero. Y lo mejor de todo, es que parece que está funcionando."

http://www.rediris.es/sir/

Edificio CICA, Campus Universitario
Avenida Reina Mercedes s/n
41012 Sevilla. España

Tel.: 95 505 66 00
Fax: 95 505 66
www.red.es
www.rediris.es