Tengo un IdP ¿y ahora qué?

de *"tenemos que montar un directorio"* a la federación global

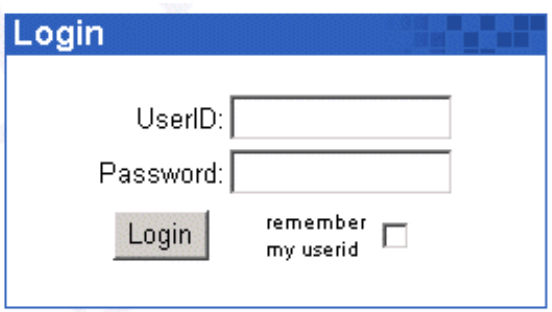
Victoriano Giralt

Servicio Central de Informática
Universidad de Málaga

4º encuentro
Gestión de Accesos e Identidades
Madrid, 7 de octubre de 2010

IdP

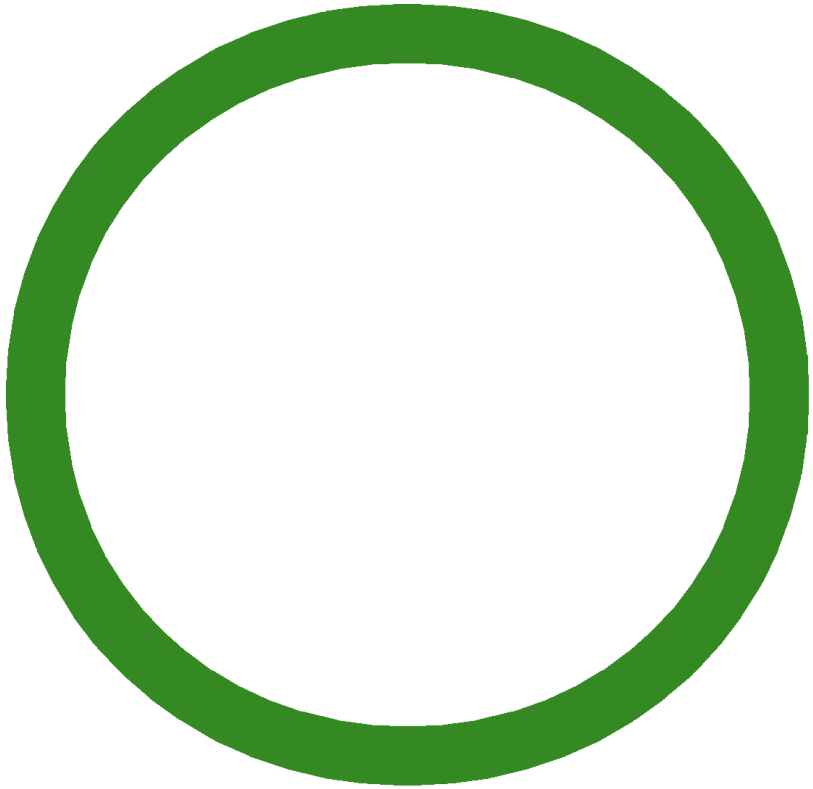
Podemos autenticar usuarios y enviar atributos



iiR España
Know-how. People. Results.

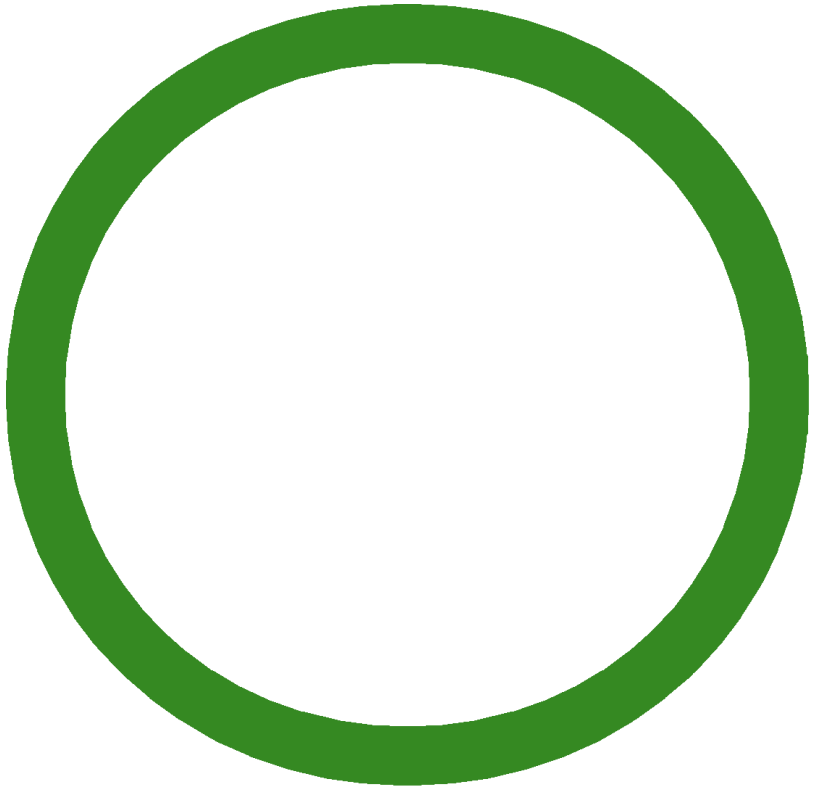
Nos podemos federar

Nos podemos federar



iiR España
Know-how. People. Results.

Nos podemos federar



confianza

¿Qué ganamos federándonos?

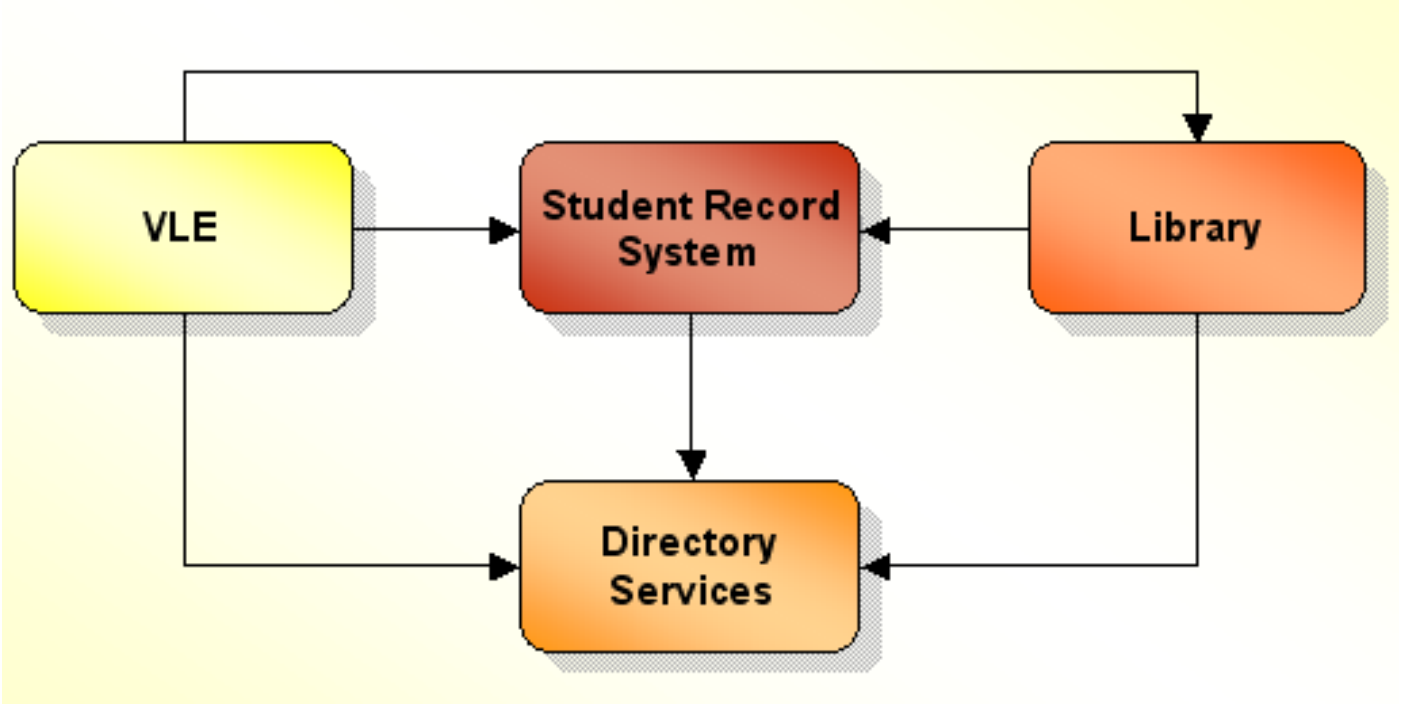
- Una mejor y más escalable gestión de accesos
- Una mejor y más escalable gestión de identidades
- Más servicios para los usuarios
- Más usuarios para los servicios
- Mejores servicios

La vision

¿Por qué la identidad federada
es importante en la Universidad?

Un ideal

Integración de aplicaciones de negocio para las Universidades



¿De verdad es tan importante la identidad?

Dos caras de la misma moneda

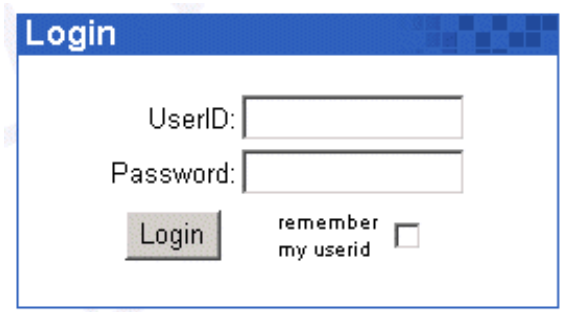
La identidad puede ser

- Una maldición $=>$ anonimato
- Una bendición $=>$ verificación de identidad

¿Qué es una identidad?

en un mundo digital

Un conjunto de credenciales y un conjunto de atributos



iiR España
Know-how. People. Results.

La edad de piedra de la autenticación

- No existía un repositorio central de credenciales
- Cada aplicación tenía el suyo propio
- Los usuarios sufrían la peor de las pesadillas

La identidad estaba muy enferma,
estaba totalmente fragmentada

La ilustración de la autenticación

HAY un directorio

- Aparecen los directorios
- Tenemos un repositorio *centralizado* para las credenciales
- En realidad, no sabemos que hacer con él
- Cada aplicación maneja su propia autenticación
- Por suerte, los usuarios solo tienen que recordar un juego de credenciales

Los fragmentos de la identidad vuelven a estar juntos

La identidad en peligro

La reunificación de la identidad la hace vulnerable

El principio del mínimo privilegio

o la parábola de la pareja

El principio del mínimo privilegio

o la parábola de la pareja

Reparto

El principio del mínimo privilegio

o la parábola de la pareja

Reparto

El usuario

El principio del mínimo privilegio

o la parábola de la pareja

Reparto

El directorio

El principio del mínimo privilegio

o la parábola de la pareja

Reparto

La aplicación

El principio del mínimo privilegio

o la parábola de la pareja

El principio del mínimo privilegio

o la parábola de la pareja

La trama

El principio del mínimo privilegio

o la parábola de la pareja

La trama

iiR España
Know-how. People. Results.

El principio del mínimo privilegio

o la parábola de la pareja

La trama

⇒

El usuario le da sus credenciales a la aplicación

El principio del mínimo privilegio

o la parábola de la pareja

La trama

⇒

⇒

La aplicación le da las credenciales del usuario al directorio

El principio del mínimo privilegio

o la parábola de la pareja

La trama

⇒

⇒

⇐

La aplicación accede con los privilegios del usuario

El principio del mínimo privilegio

o la parábola de la pareja

La trama

⇒
⇐

⇒
⇐

El usuario consigue acceder a la aplicación

El principio del mínimo privilegio

o la parábola de la pareja

La trama

$\Rightarrow$
$\Leftarrow$

$\Rightarrow$
$\Leftarrow$

Todos están contentos

El principio del mínimo privilegio

o la parábola de la pareja

La trama

⇒
⇐

⇒
⇐

Todos están contentos ¿seguro?

El principio del mínimo privilegio

o la parábola de la pareja

El principio del mínimo privilegio

o la parábola de la pareja

Una trama mejor

El principio del mínimo privilegio

o la parábola de la pareja

Una trama mejor

El principio del mínimo privilegio

o la parábola de la pareja

Una trama mejor

$\Rightarrow$

El usuario le da sus credenciales a la aplicación

El principio del mínimo privilegio

o la parábola de la pareja

Una trama mejor

⇒

⇒

La aplicación le da sus credenciales al directorio

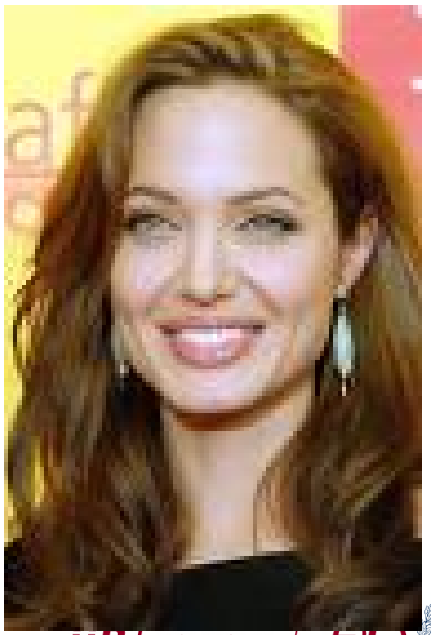
El principio del mínimo privilegio

o la parábola de la pareja

Una trama mejor

⇒

⇒
⇐



La aplicación obtiene acceso de aplicación al directorio

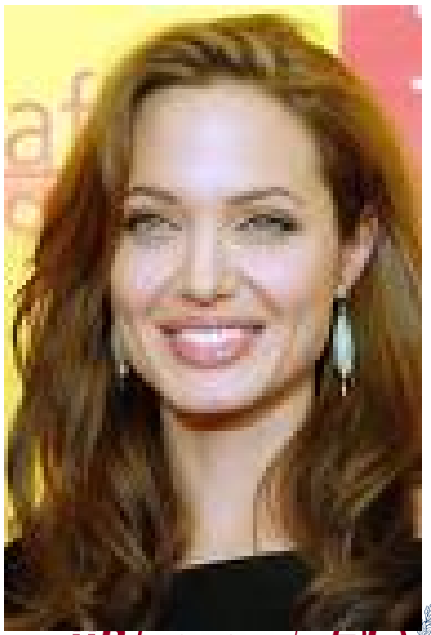
El principio del mínimo privilegio

o la parábola de la pareja

Una trama mejor

⇒

⇒
⇐
⇒
⇐



Directorio y aplicación verifican las credenciales del usuario

El principio del mínimo privilegio

o la parábola de la pareja

Una trama mejor

⇒
⇐

⇒
⇐
⇒
⇐

El usuario consigue acceso a la aplicación

El principio del mínimo privilegio

o la parábola de la pareja

Una trama mejor

⇒
⇐

⇒
⇐
⇒
⇐

Todos contentos

El principio del mínimo privilegio

o la parábola de la pareja

Una trama mejor

⇒
⇐

⇒
⇐
⇒
⇐

Todos contentos, ¿no?...

El principio del mínimo privilegio

o la parábola de la pareja

Una trama mejor

⇒
⇐

⇒
⇐
⇒
⇐

La aplicación tiene acceso a las credenciales del usuario

El principio del mínimo privilegio

o la parábola de la pareja

Una trama mejor

⇒
⇐

⇒
⇐
⇒
⇐

¿Nos podemos fiar de nuestra aplicaciones?

El principio del mínimo privilegio

o la parábola de la pareja

Una trama mejor

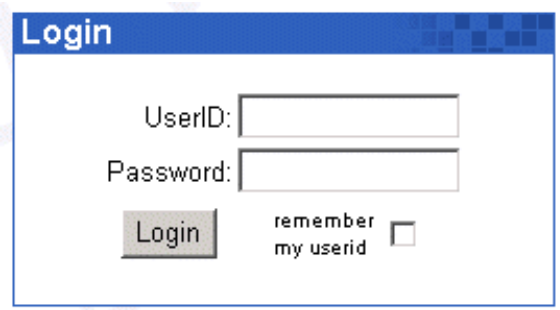
⇒
⇐

⇒
⇐
⇒
⇐

¿Nos podemos fiar de nuestra aplicaciones? ¿de todas?

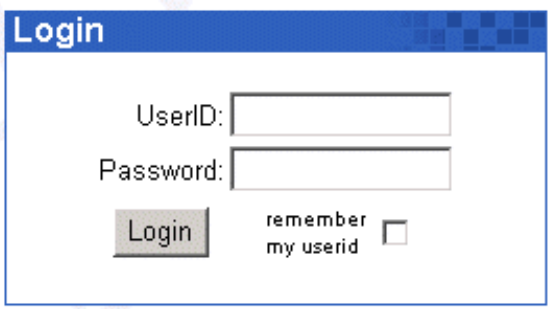
Un punto único de autenticación

Podemos proteger las credenciales y los atributos



Un punto único de autenticación

Podemos educar a los usuarios



Repensando el modelo

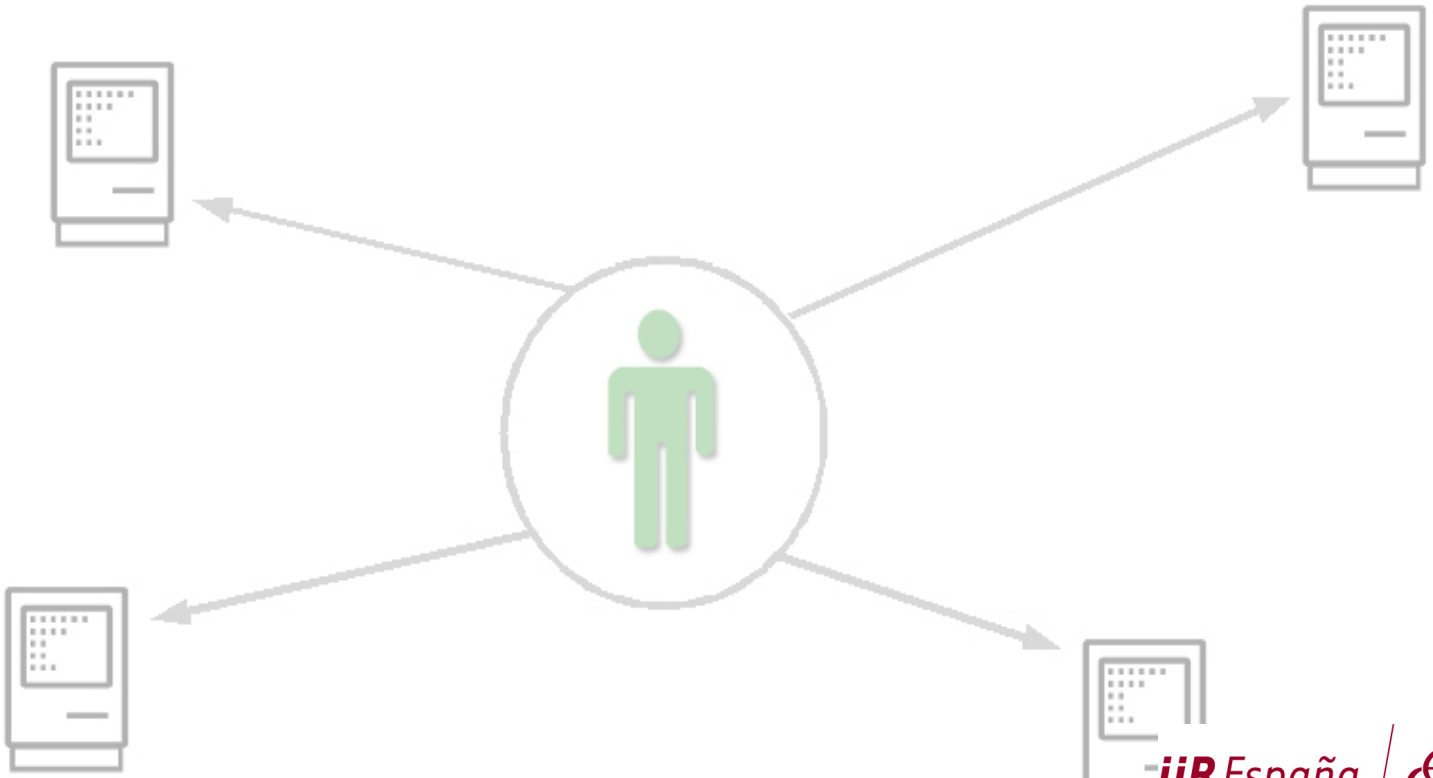
Necesitamos un nuevo paradigma

Modelo antiguo

habitaciones y paredes

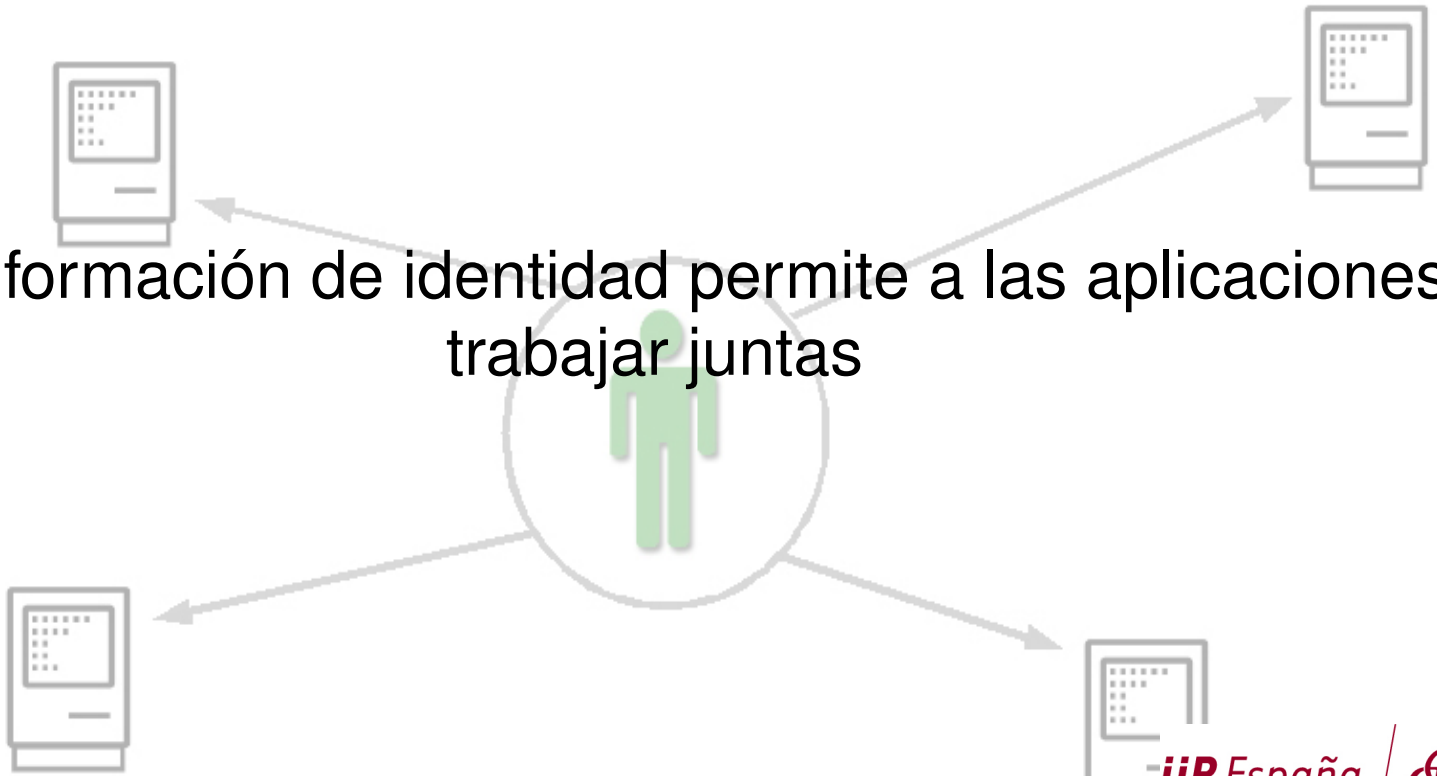
La Identidad como servicio

Aplicaciones centradas en el usuario



La Identidad como servicio

Aplicaciones centradas en el usuario



Un nuevo modelo

un espacio abierto y continuo

Requisitos

los planos para nuestro loft

Requisitos

los planos para nuestro loft

Nuestras aplicaciones deberían

Requisitos

los planos para nuestro loft

Nuestras aplicaciones deberían

- Colaborar entre ellas
- Estar centradas en el usuario
- Reducir la carga sobre el usuario
- Integrar los datos corporativos
- Tener en cuenta la experiencia previa del usuario
- Ser las mejores para cada servicio
- Rebajar el *escalón* de acceso

Colaboración

usar la identidad para poner al usuario a los mandos

Interoperability is the degree to which a provider and a consumer can succesfully interface having never met

Coppeto, T.: Introduction To OSID V3 for developers

El *cluster* de aplicaciones del SCI

Herramientas para la colaboración

Nuestro objetivo es que los grupos trabajen juntos

El *cluster* de aplicaciones del SCI

Herramientas para la colaboración

Nuestro objetivo es que los grupos trabajen juntos

- Gestión de grupos
- Wiki
- Blog
- Lista de correo
- Foros Web
- Chat
- Compartición de fichero vía Web
- ...

sin olvidar el acceso a aplicaciones corporativas

El *cluster* de aplicaciones del SCI

Herramientas para la colaboración

Nuestro objetivo es que los grupos trabajen juntos

- Gestión de grupos
- Wiki
- Blog
- Lista de correo
- Foros Web
- Chat
- Compartición de fichero vía Web
- ...

sin olvidar el acceso a aplicaciones corporativas
todos ellos con las mismas credenciales

El *cluster* de aplicaciones del SCI

Herramientas para la colaboración

Nuestro objetivo es que los grupos trabajen juntos

- Gestión de grupos
- Wiki
- Blog
- Lista de correo
- Foros Web
- Chat
- Compartición de fichero vía Web
- ...

sin olvidar el acceso a aplicaciones corporativas
mejor, todos ellos compartiendo la misma sesión

Persiguiendo un ideal

Persiguiendo un ideal

Un camino largo y serpenteante

Persiguiendo un ideal

Un camino largo y serpenteante

Persiguiendo un ideal

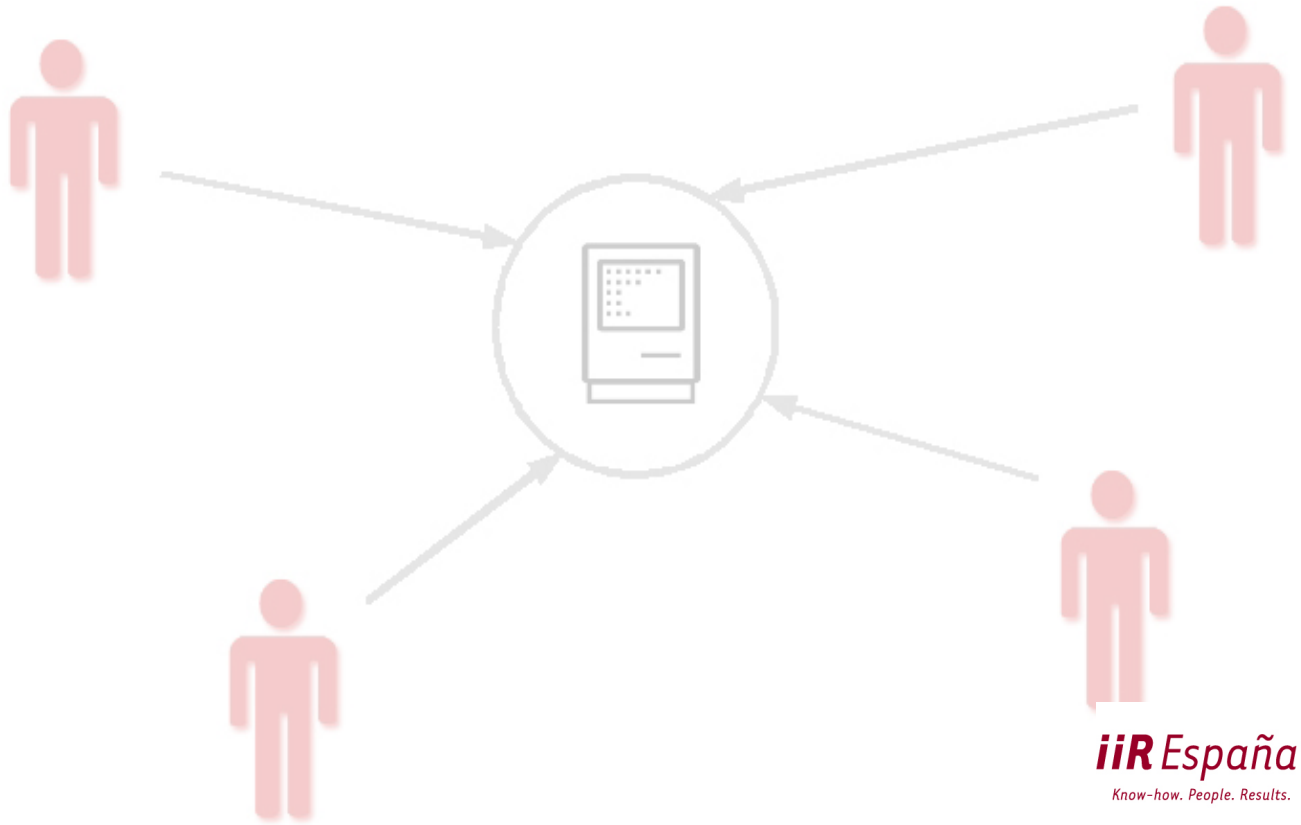
Un camino largo y serpenteante

Persiguiendo un ideal

creímos atravesar las puertas del Infierno

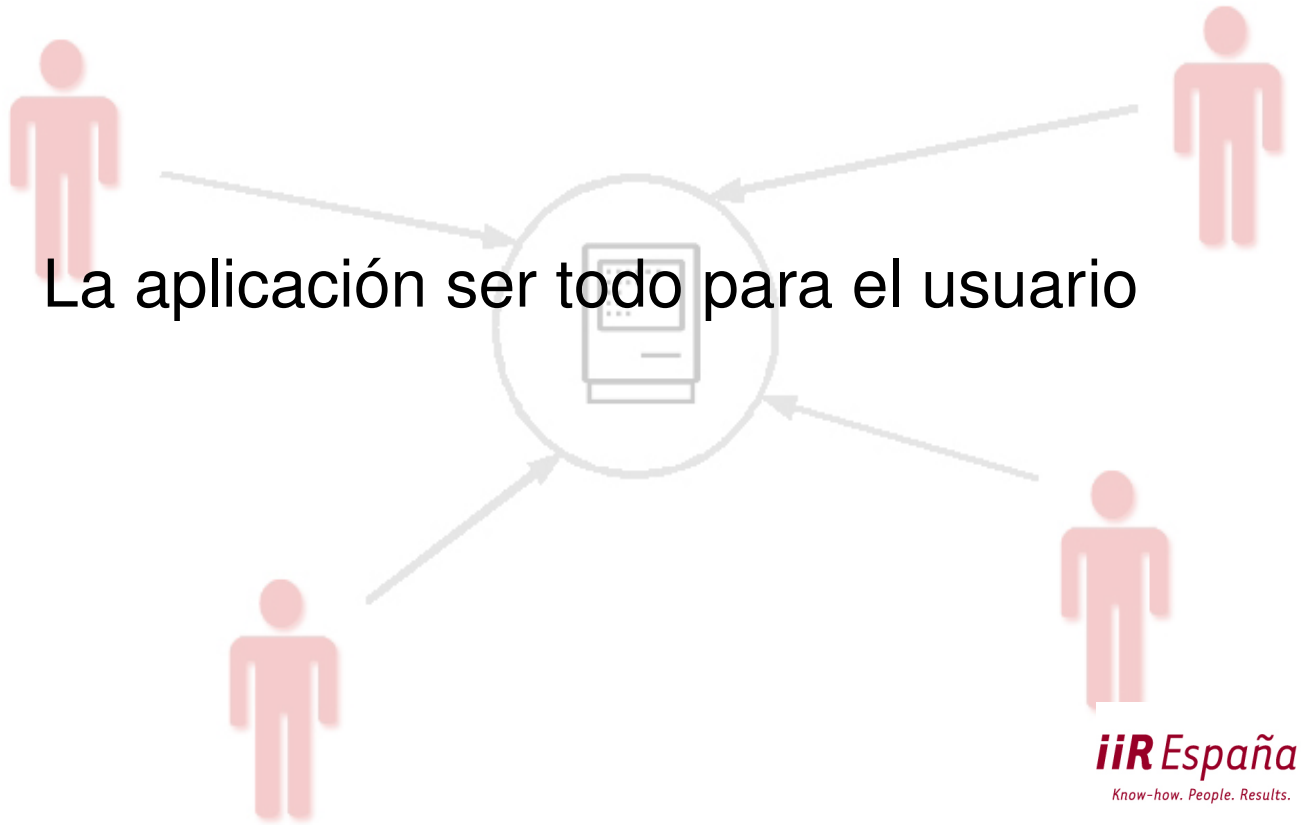
Centrados en la aplicación

El paradigma de la plataforma monolítica



Centrados en la aplicación

El paradigma de la plataforma monolítica



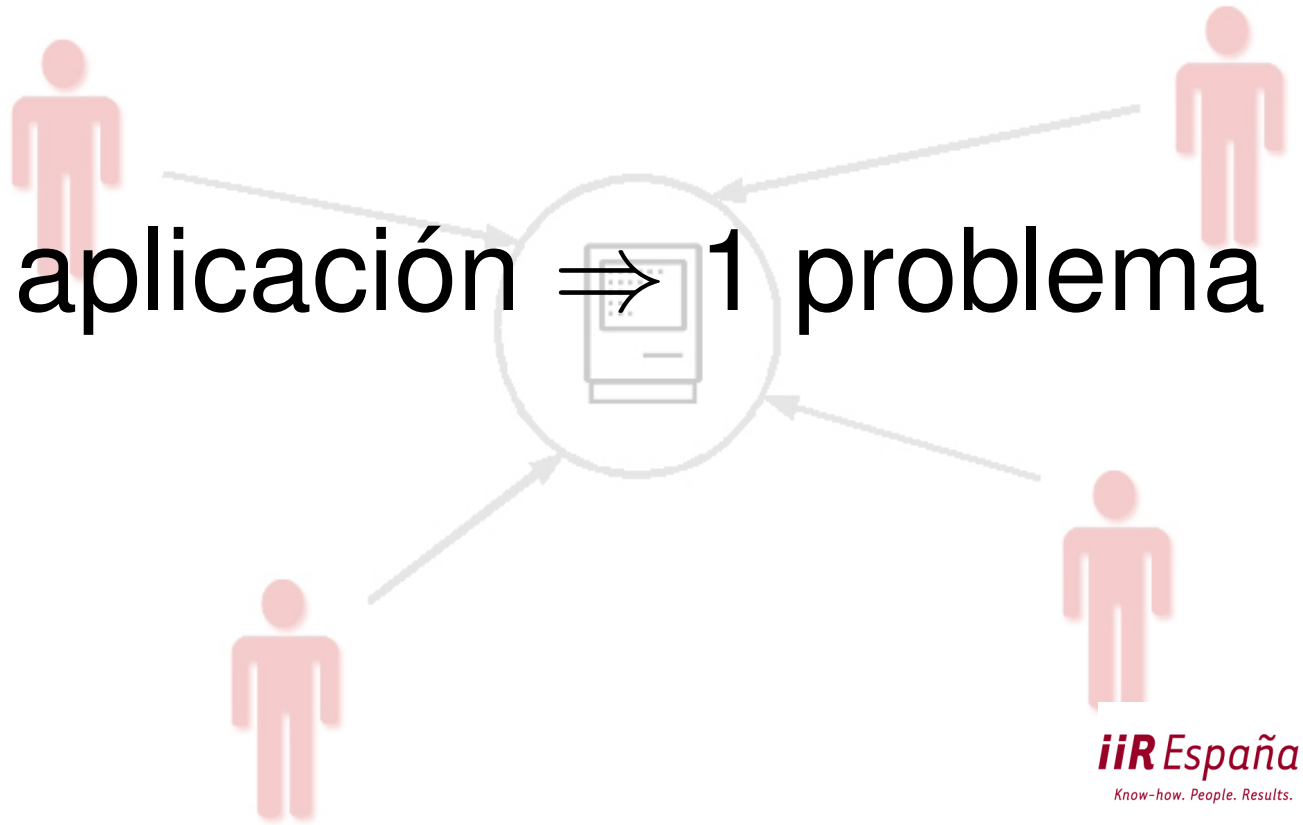
La carrera de las prestaciones

una huida hacia ninguna parte

Caso severo de inflamación de opciones (*featuritis*)

Las plataformas o *suites*

la solución a nuestros problemas



1 aplicación $\Rightarrow$ 1 problema

Las plataformas o *suites*

¿la solución a nuestros problemas?

Las aplicaciones tienen *su* carácter

Las plataformas o *suites*

¿la solución a nuestros problemas?

La mejor forma de hacer las cosas

Las plataformas o *suites*

¿la solución a nuestros problemas?

La mejor forma de hacer las cosas

Las plataformas o *suites*

¿la solución a nuestros problemas?

La mejor forma de hacer las cosas

La mía

Provisión

ajustando nuestros procesos *al carácter*

Es posible acceder a los deseos de la aplicación

Provisión

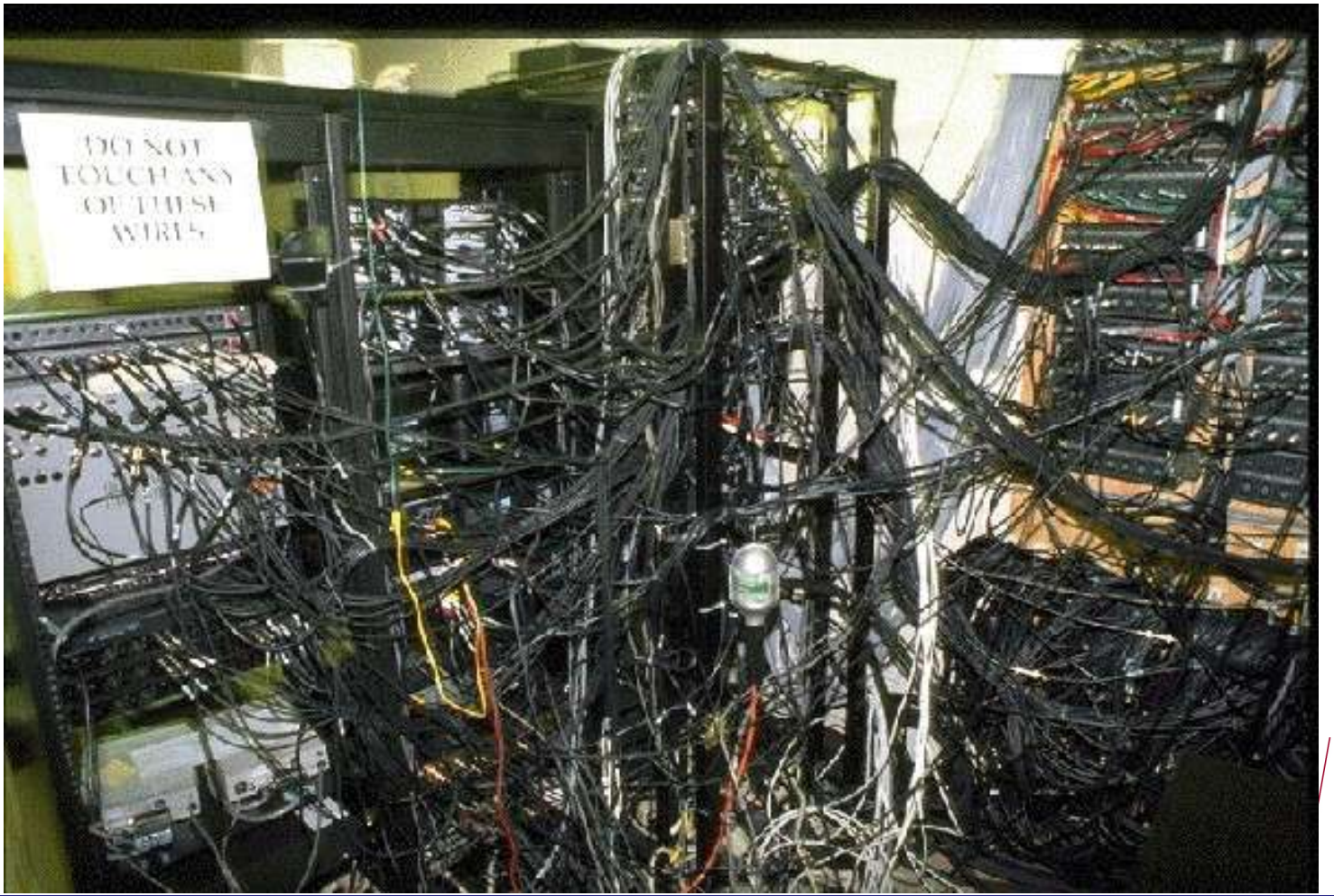
ajustando nuestros procesos *al carácter*

Es posible acceder a los deseos de la aplicación

- Desarrollando estrategias de provisión
- Usando tecnologías no demasiado extendidas
- Emitiendo conjuros arcanos
- ...

Provisión

ajustando nuestros procesos *al carácter*



¿Estamos perdidos?

¿Qué pueden hacer los administradores y los desarrolladores?

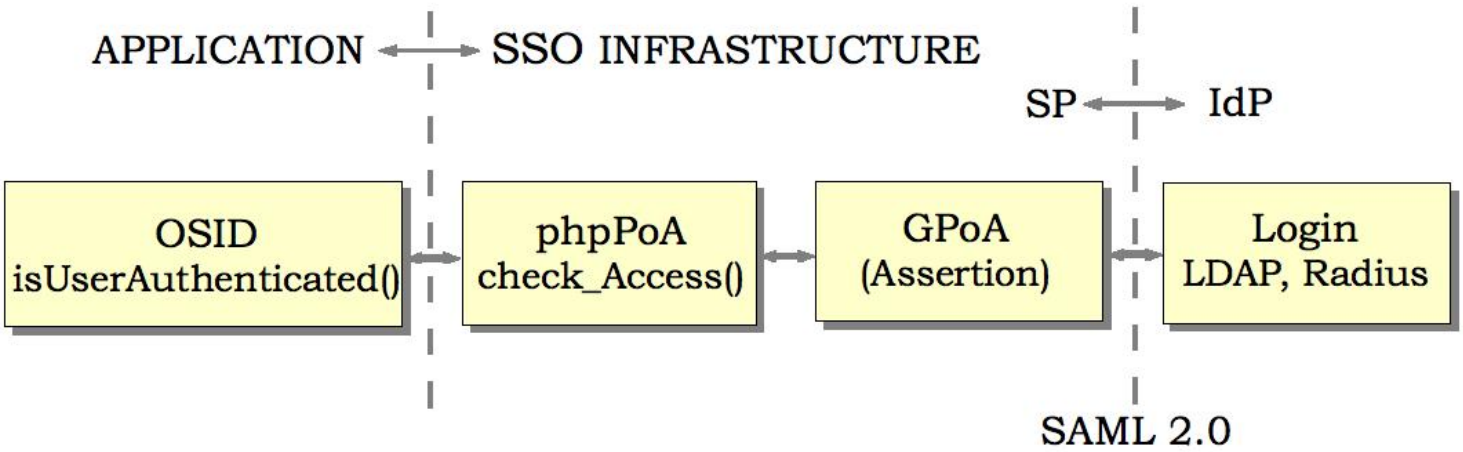
FIAM

La identidad federada al rescate

iiR España
Know-how. People. Results.

Una arquitectura de Autenticación y Autorización

independiente de mecanismos



El pegamento

que mantiene unidas las piezas

El pegamento

que mantiene unidas las piezas

Hemos desarrollado un marco mínimo
para integrar aplicaciones

El pegamento

que mantiene unidas las piezas

Hemos desarrollado un marco mínimo
para integrar aplicaciones

- Mínimamente invasivo
- Operaciones comunes
  - ¿Está autenticado el usuario?
  - autenticar al usuario
  - obtener atributos
  - cerrar la sesión
- con transportes de identidad intercambiables

Pegas

que hemos encontrado en nuestra búsqueda

Pegas

que hemos encontrado en nuestra búsqueda

Nos hemos dado unos cuantos coscorrones por el camino

Pegas

que hemos encontrado en nuestra búsqueda

Nos hemos dado unos cuantos coscorrones por el camino

- Peleas de sesiones
- Salpicón de cookies
- Despensas de usuarios
- Revuelto de código
- Código cerrado
- ...

Hemos conseguido unos cuantos objetivos

Hemos conseguido unos cuantos objetivos

Hay luz al final del túnel

Hemos conseguido unos cuantos objetivos

la joya de la corona

Hemos conseguido unos cuantos objetivos

la joya de la corona

Un panel de gestión de la identidad

Hemos conseguido unos cuantos objetivos

la joya de la corona

Un panel de gestión de la identidad

Hemos conseguido unos cuantos objetivos

la joya de la corona

Un panel de gestión de la identidad, con autoservicio

Hemos conseguido unos cuantos objetivos

Hemos conseguido unos cuantos objetivos

Ahora

Hemos conseguido unos cuantos objetivos

Ahora

- Tenemos un buen puñado de aplicaciones trabajando juntas
- Podemos incorporar usuarios externos con facilidad
- Podemos conectarnos fácilmente a servicios de otros
- Somos parte de un campus virtual de 10 universidades

Herramientas

Nos han ayudado bastante

- SAML
- Simple SAML php
- Shibboleth
- memcached
- Django
- Sympa
- MediaWiki
- DokuWiki
- OIOSAML
- ...

Facilitadores

Los principales ingredientes de nuestra levadura

- Aplicaciones de código abierto
- Trabajar con la comunidad

Facilitadores

Los principales ingredientes de nuestra levadura

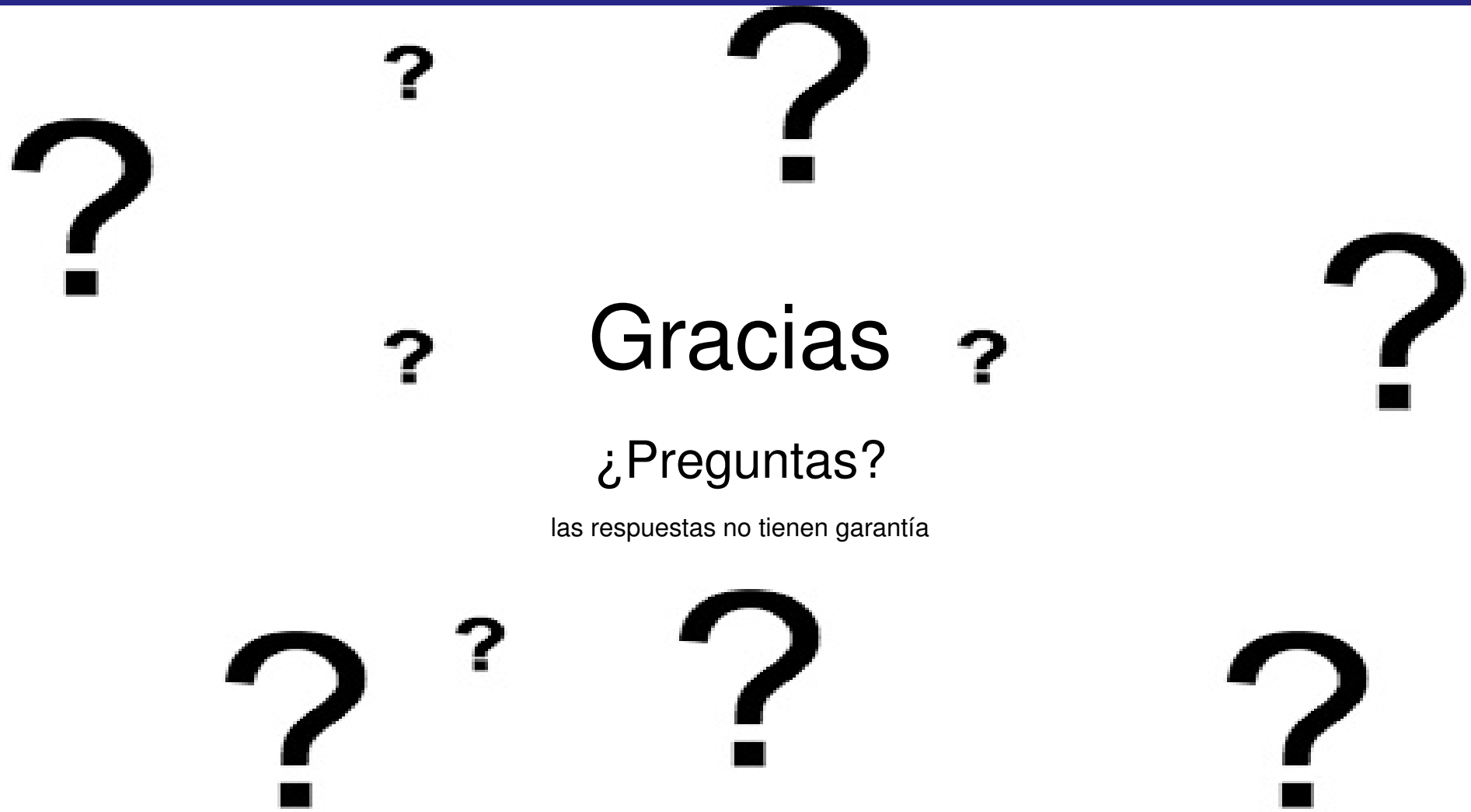
- Aplicaciones de código abierto
- Trabajar con la comunidad
- La autenticación HTTP basic
- Las APIs de provisión

Cosas que faltan

Necesitamos

- Desacoplar los usuarios
- Autorización externa
- Olvidarnos de la provisión
- Buena gestión de grupos
- Gestión de la colaboración:
  Entornos Virtuales $\rightarrow$ Organizaciones que colaboran
- Un buen proceso de Logout
- Salirnos de la web

Gracias



Gracias

¿Preguntas?

las respuestas no tienen garantía