Estándares de gestión de identidades y accesos Identidad federada

la experiencia de la UMA

Victoriano Giralt

Servicio Central de Informática
Universidad de Málaga

Madrid
20 de mayo 2009

Gatear
hoy empieza todo

Gatear
hoy empieza todo

Queremos gestionar la identidad

- Orígenes de autoridad
- Tipos de personas
- Almacen de identidades
- Estándares

Orígenes de autoridad

¿Dónde está mi gente?

“”La fragmentación de identidad es el cáncer del IAM“”(Keith Hazelton)

Es fundamental disponer de un código unívoco y diferenciado para enlazar las entradas del directorio con las entradas origen en los sistemas de registro.

que pueden ser muchos

Tipos de personas

Clasificar para saber

Es necesario conocer las relaciones con la institución, y de dónde vienen

Tipos de personas

Clasificar para saber

Es necesario conocer las relaciones con la institución, y de dónde vienen

- PAS

Tipos de personas

Clasificar para saber

Es necesario conocer las relaciones con la institución, y de dónde vienen

- PAS ¿PAS investigador?

Tipos de personas

Clasificar para saber

Es necesario conocer las relaciones con la institución, y de dónde vienen

- PAS ¿PAS investigador? la última moda

Tipos de personas

Clasificar para saber

Es necesario conocer las relaciones con la institución, y de dónde vienen

- PAS ¿PAS investigador? la última moda
- PDI

Tipos de personas

Clasificar para saber

Es necesario conocer las relaciones con la institución, y de dónde vienen

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios?

Tipos de personas

Clasificar para saber

Es necesario conocer las relaciones con la institución, y de dónde vienen

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos?

Tipos de personas

Clasificar para saber

Es necesario conocer las relaciones con la institución, y de dónde vienen

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC?

Tipos de personas

Clasificar para saber

Es necesario conocer las relaciones con la institución, y de dónde vienen

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC? . . .

Tipos de personas

Clasificar para saber

Es necesario conocer las relaciones con la institución, y de dónde vienen

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC? . . .
- Alumnos

Tipos de personas

Clasificar para saber

Es necesario conocer las relaciones con la institución, y de dónde vienen

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC? . . .
- Alumnos ¿ciclo?

Tipos de personas

Clasificar para saber

Es necesario conocer las relaciones con la institución, y de dónde vienen

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC? . . .
- Alumnos ¿ciclo? ¿movilidad?

Tipos de personas

Clasificar para saber

Es necesario conocer las relaciones con la institución, y de dónde vienen

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC? . . .
- Alumnos ¿ciclo? ¿movilidad?
- Eméritos
- Colaboradores
- Inclasificables

Tipos de personas

Clasificar para saber

Es necesario conocer las relaciones con la institución, y de dónde vienen

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC? . . .
- Alumnos ¿ciclo? ¿movilidad?
- Eméritos
- Colaboradores
- Inclasificables

¿de quién . . . es esta dirección de correo?

Almacen de identidades

¿Dónde guardo a mi gente? ¿Cómo la guardo?

El directorio es la piedra angular de la Identidad

Almacen de identidades

¿Dónde guardo a mi gente? ¿Cómo la guardo?

El directorio es la piedra angular de la Identidad

- Árbol somero

Menos ramas, menos problemas

Estableciendo una rama
para cada tipo de objeto (pocos)
la administración se simplifica.
Los objetos no suelen cambiar de tipo.

Almacen de identidades

¿Dónde guardo a mi gente? ¿Cómo la guardo?

El directorio es la piedra angular de la Identidad

- Árbol somero
- Rama única para personas

Las personas son personas

Independientemente de
su relación con la institución
en un determinado momento.
Y no es raro que tengan
varios tipos de relación.

Almacen de identidades

¿Dónde guardo a mi gente? ¿Cómo la guardo?

El directorio es la piedra angular de la Identidad

- Árbol somero
- Rama única para personas
- Clasificaciones

Jerarquías superpuestas

Asignando códigos de clasificación,
un mismo objeto,
puede situarse en diversos lugares
dentro de jerarquías diferentes, incluso,
dentro de la misma jerarquía.

Almacen de identidades

¿Dónde guardo a mi gente? ¿Cómo la guardo?

El directorio es la piedra angular de la Identidad

- Árbol somero
- Rama única para personas
- Clasificaciones
- Privacidad

DNs opacos

Para evitar la fuga de datos personales, usamos DNs compuestos opacos, así no se pueden asociar a las personas a simple vista.

Almacen de identidades

¿Dónde guardo a mi gente? ¿Cómo la guardo?

El directorio es la piedra angular de la Identidad

- Árbol somero
- Rama única para personas
- Clasificaciones
- Privacidad

Mis datos son mios

Un atributo de control de privacidad, permite a los usuarios controlar la publicación de su información, accesible de forma abierta a cualquiera.

Almacen de identidades

¿Dónde guardo a mi gente? ¿Cómo la guardo?

El directorio es la piedra angular de la Identidad

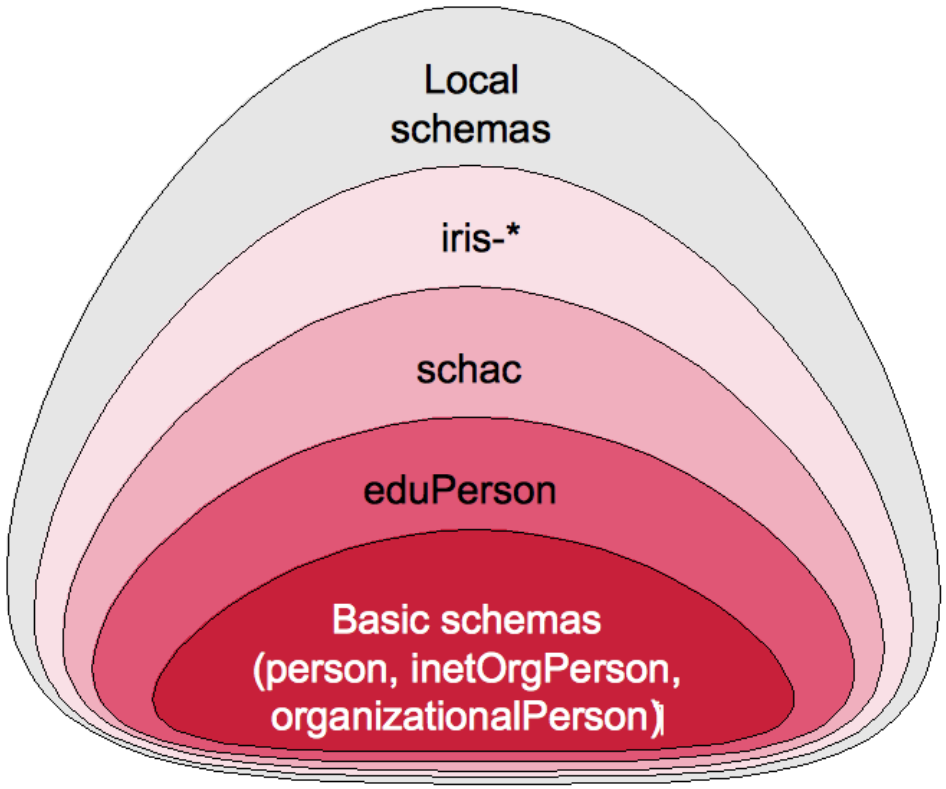
- Árbol somero
- Rama única para personas
- Clasificaciones
- Privacidad
- Autorizaciones

Quién hace qué

Mantener los permisos con
la descripción de la persona
permite desacopar las autorizaciones.

Estándares
no es necesario reinventar la rueda

Otros pueden tener mis mismos problemas



Andar
interaccionando con los amigos

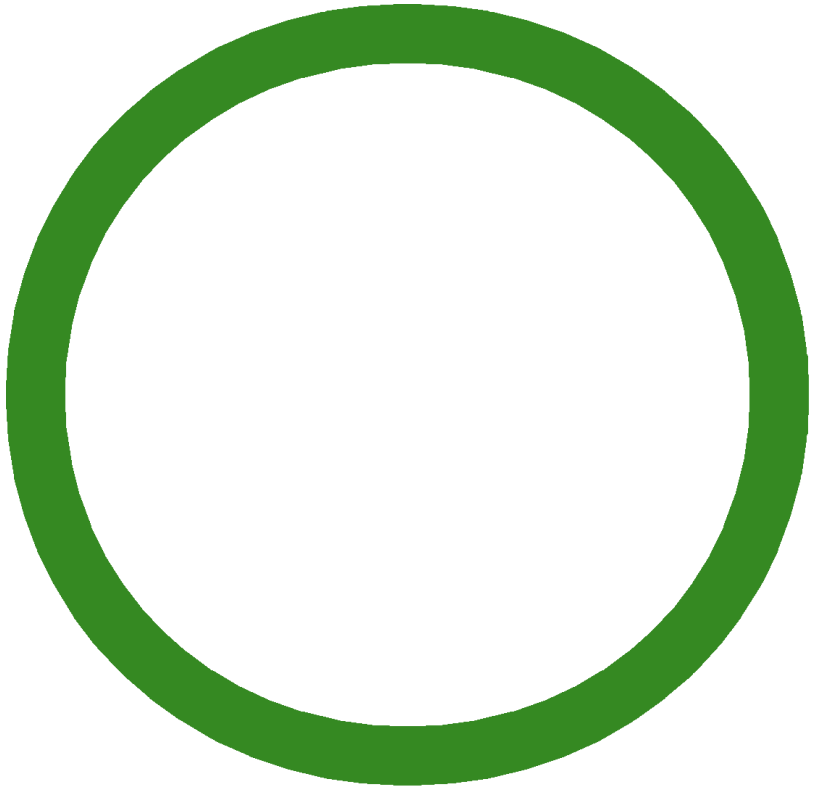
- Motivos
- Definiciones
- Lenguaje
- Modelos

Federación

¿Qué es una federación?

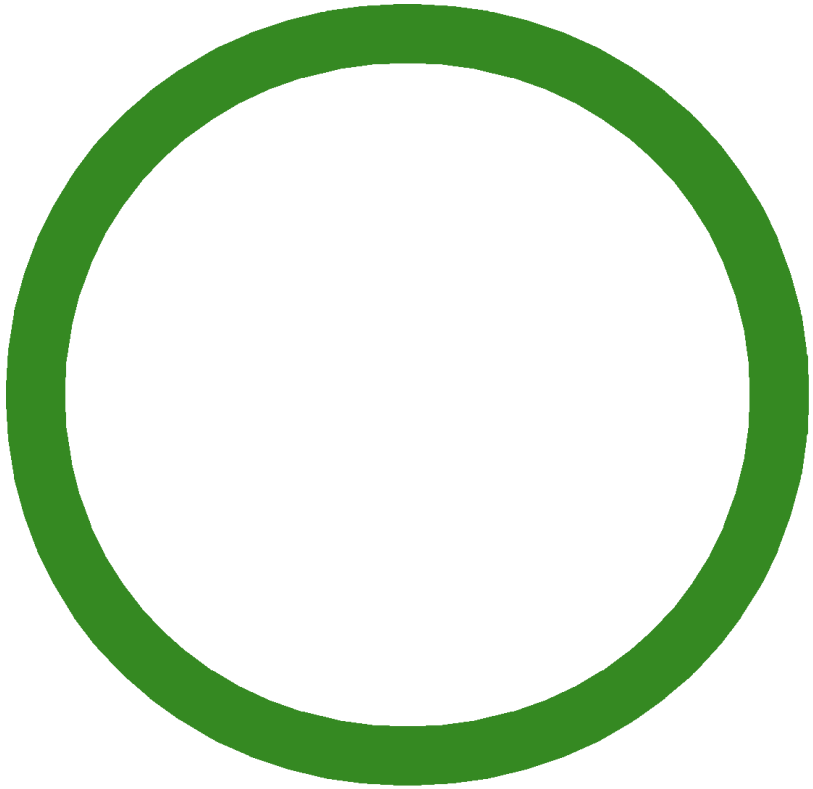
Federación

¿Qué es una federación?



Federación

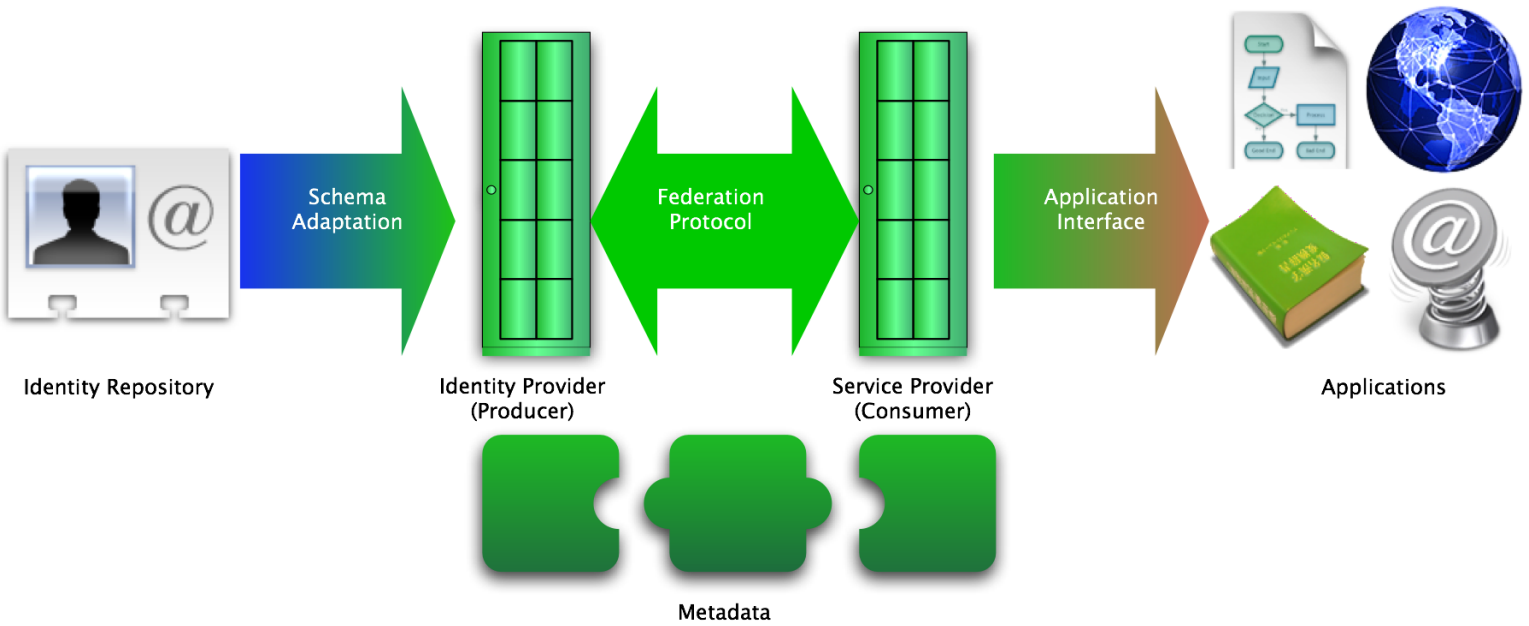
¿Qué es una federación?



de confianza

Federación

¿Qué es una federación?



Federar
¿Qué nos aporta?

Los objetivos de la federación

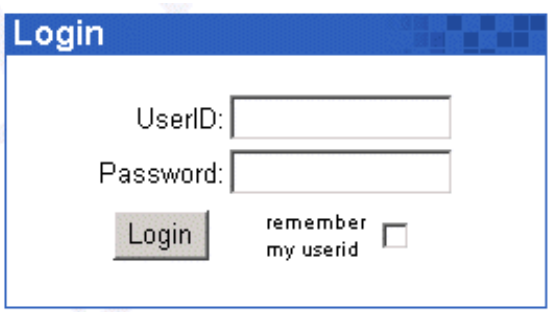
- Mejor gestión de accesos y escalable
- Mejor gestión de identidad y escalable
- Más servicios para los usuarios
- Más usuarios para los servicios
- Mejores servicios

Un caso de éxito

Nace la mayor federación del mundo

IdP
Identity Provider

Una entidad de autenticación y liberación de atributos



SP
Service Provider

Una entidad que consume atributos

Comunicarse

es necesario un lenguaje común

Comunicarse
es necesario un lenguaje común

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

Para conseguir ésto, las partes necesitan un lenguaje común con sintáxis y semántica que entiendan todas.

Los esquemas comunes son el punto de inicio.

SAML

La *lingua franca* de las federaciones

Security Assertion Markup Language

- Aserciones

Información sobre autenticación, atributos y autorización

SAML

La *lingua franca* de las federaciones

Security Assertion Markup Language

- Aserciones
- Protocolos

Elementos de petición y respuesta que empaquetan las aserciones

SAML
La *lingua franca* de las federaciones

Security Assertion Markup Language

- Aserciones
- Protocolos
- Bindings

Cómo se asocian los protocolos SAML con protocolos de transporte

SAML
La *lingua franca* de las federaciones

Security Assertion Markup Language

- Aserciones
- Protocolos
- Bindings
- Perfiles

Cómo se combinan los bindings, protocolos y aserciones SAML para un caso de uso concreto

Terminología legal
el pegamento de las federaciones

Las federaciones son más legales que técnicas, es “el zoo de los papeles” (David Simonsen)

- Política de la federación
  - Criterios de pertenencia
  - Mecanismos de funcionamiento
  - Uso aceptable

Terminología legal
el pegamento de las federaciones

Las federaciones son más legales que técnicas, es “el zoo de los papeles” (David Simonsen)

- Política de la federación
- Contratos

- Bilateral
- Personas jurídicas
- Deberes
- Responsabilidades
- Foro

Terminología legal
el pegamento de las federaciones

Las federaciones son más legales que técnicas, es "el zoo de los papeles" (David Simonsen)

- Política de la federación
- Contratos
- Attribute Release Policy

Qué datos personales obtiene el servicio

Terminología legal
el pegamento de las federaciones

Las federaciones son más legales que técnicas, es “el zoo de los papeles” (David Simonsen)

- Política de la federación
- Contratos
- Attribute Release Policy

Principios del intercambio

- Tranparencia
- Legitimidad
- Proporcionalidad

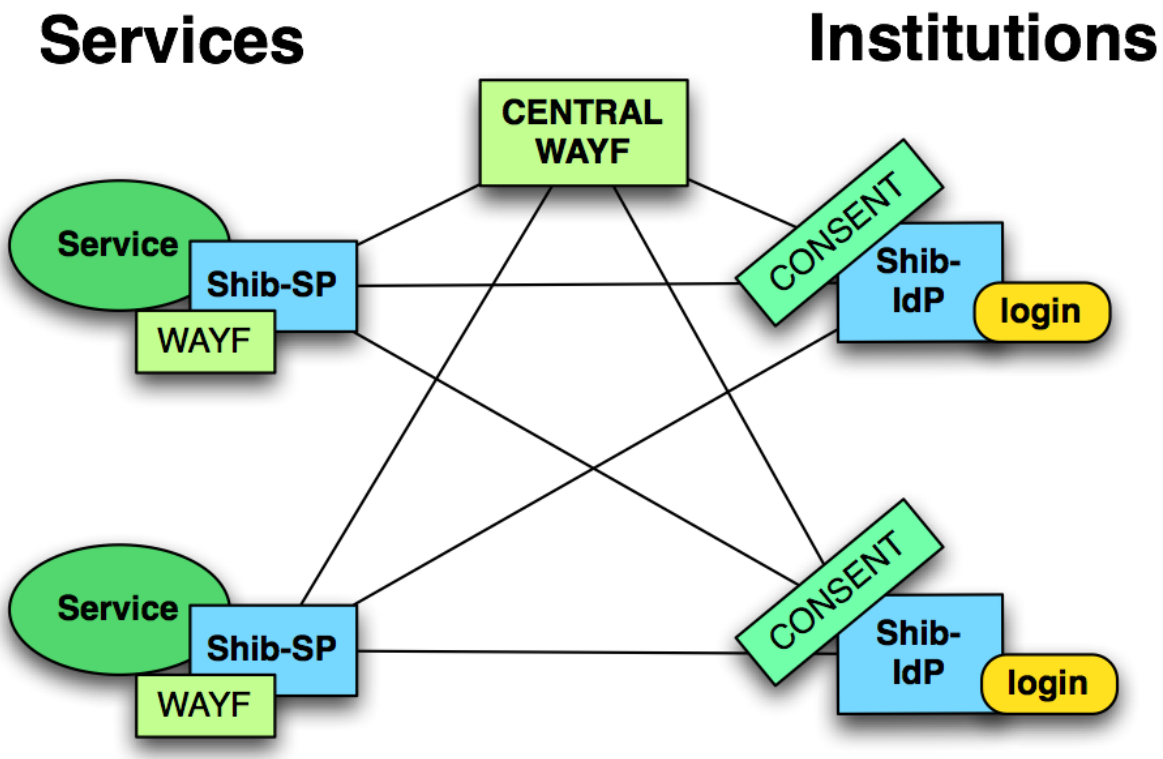
Terminología legal
el pegamento de las federaciones

Las federaciones son más legales que técnicas, es "el zoo de los papeles" (David Simonsen)

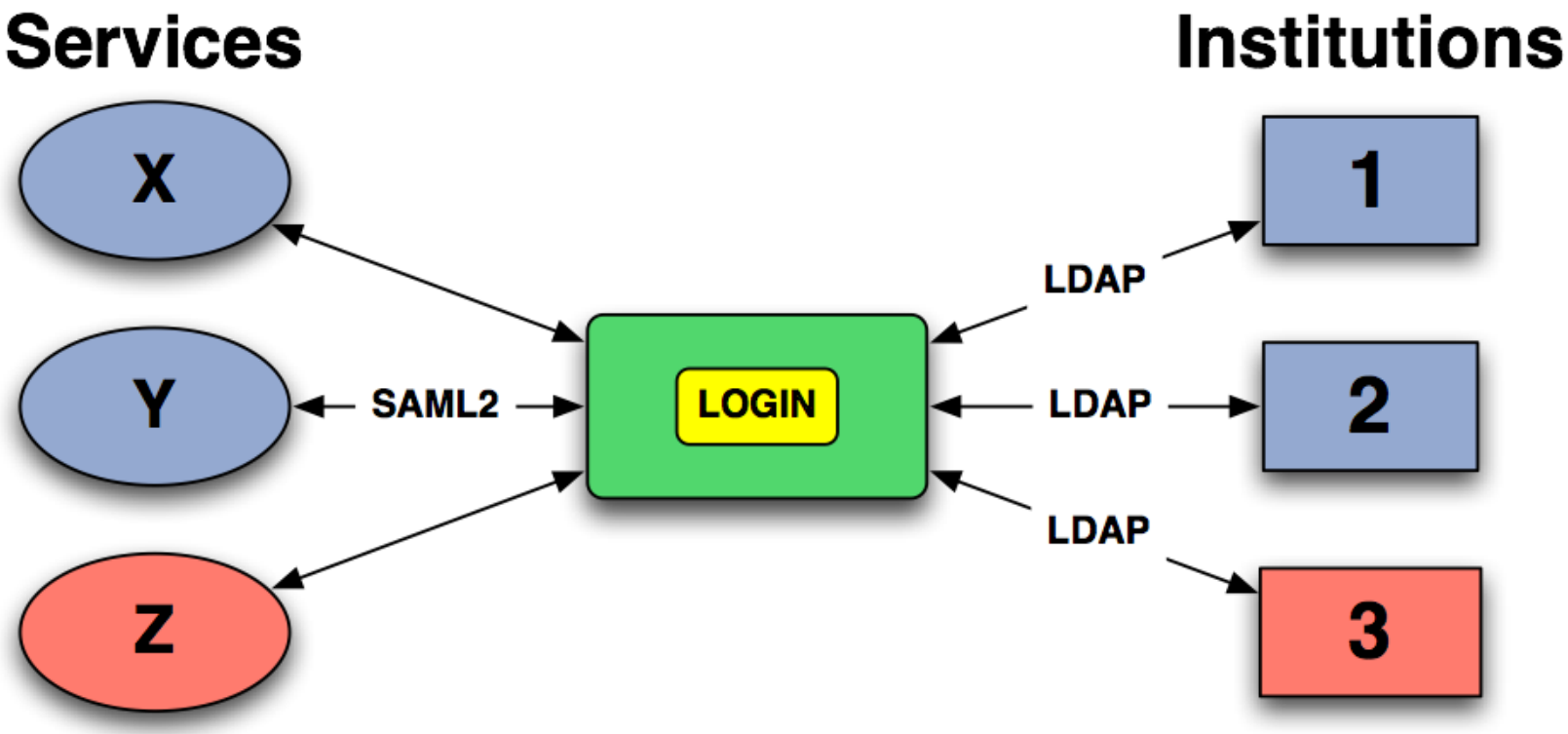
- Política de la federación
- Contratos
- Attribute Release Policy
- Consentimiento informado

Debe ser
- Voluntario
- Con un fin claro
- Comprensible

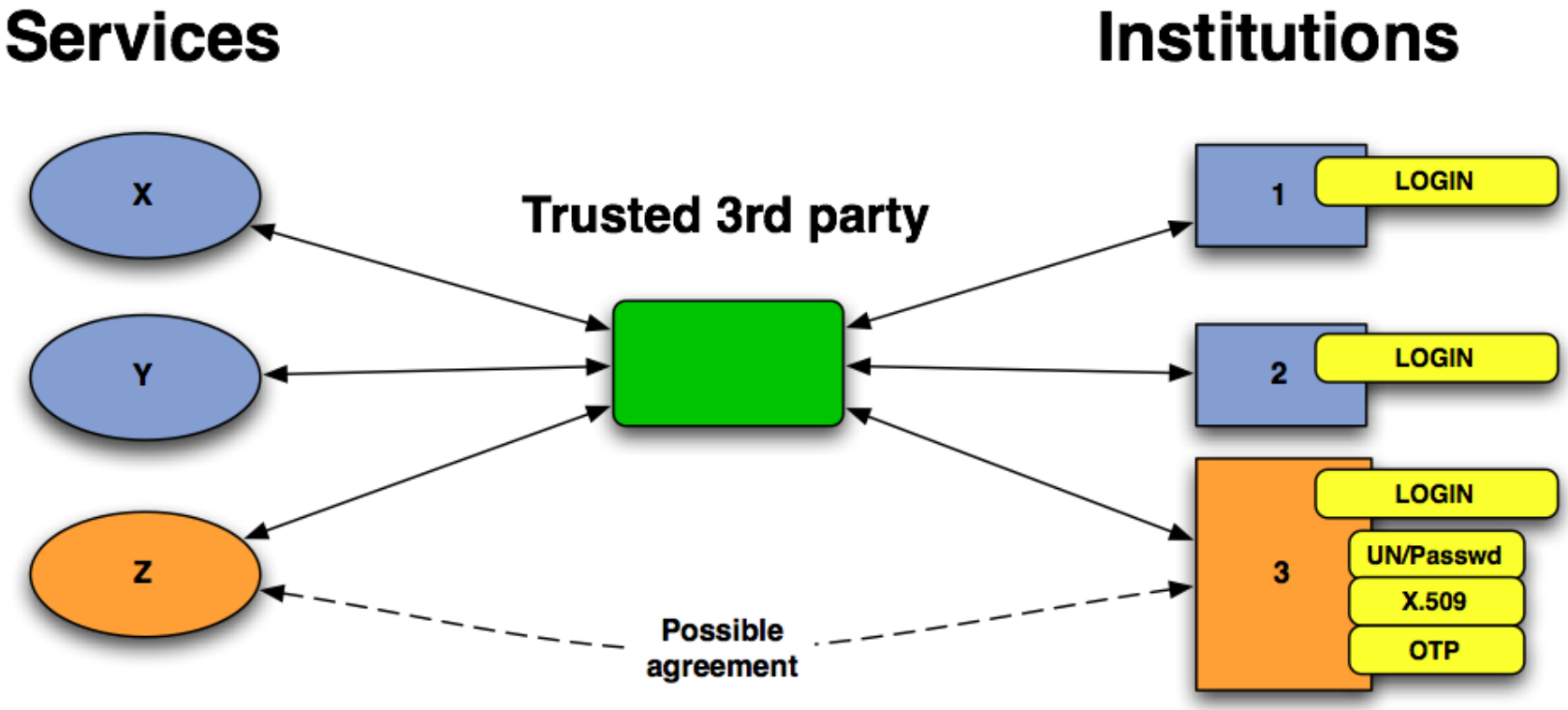
Shibboleth
el modelo distribuido



Feide
el modelo centralizado



WAYF.dk
el modelo radial



Correr
avanzado hacia el futuro

Queda mucho por hacer, mucho por cambiar

- Interfederaciones
- Aplicaciones federables
- Autorización desacoplada
- Aplicaciones centradas en la identidad
- Privacidad
- Nivel de certeza

Tropezar

Los riegos: mejor prevenir que curar

El SMTP nos trajo el *spam*, ¿qué nos traerán as federaciones?

- *Phishing*
- ¿Son seguros los certificados de cliente?
- Abuso de los contratos
- Intromisón en la privacidad
- Exceso de anonimato
- . . .