Identidad y privacidad

cómo diferenciarnos sin que se sepa quiénes somos o qué hacemos

Victoriano Giralt

Servicio Central de Informática
Universidad de Málaga

Escuela Técnica Superior de Ingeniería Informática
Málaga
14 de abril de 2011

Índice

Índice

Índice

Índice

La Identidad es escurridiza en el mundo digital

“en Internet nadie sabe que eres un perro”

¿Es tan importante la identidad?

vamos al cine ...

La gestión de identidad con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

La gestión de identidad con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

- “¡Hola! Soy María”

La gestión de identidad con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

- “¡Hola! Soy María” (*Identidad*)

La gestión de identidad con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

- “¡Hola! Soy María” (*Identidad*)
- “y aquí están mi usuario y clave para demostrarlo”

La gestión de identidad con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

- “¡Hola! Soy María” (*Identidad*)
- “y aquí están mi usuario y clave para demostrarlo” (Verificar la identidad = Autenticar = *AuthN*)

La gestión de identidad con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

- “¡Hola! Soy María” (*Identidad*)
- “y aquí están mi usuario y clave para demostrarlo” (Verificar la identidad = Autenticar = *AuthN*)
- ”Quiero entregar unos trabajos“

La gestión de identidad con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

- “¡Hola! Soy María” (*Identidad*)
- “y aquí están mi usuario y clave para demostrarlo”
  (Verificar la identidad = Autenticar = *AuthN*)
- ”Quiero entregar unos trabajos“
  (Autorizar = *AuthR*:
  Permitir a María usar los servicios
  a los que tiene derecho)

La gestión de identidad con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

- “¡Hola! Soy María” (*Identidad*)
- “y aquí están mi usuario y clave para demostrarlo”
  (Verificar la identidad = Autenticar = *AuthN*)
- ”Quiero entregar unos trabajos“
  (Autorizar = *AuthR*:
  Permitir a María usar los servicios
  a los que tiene derecho)
- ”Ya puestos me gustaría cambiarle a Juan la nota
  de Física del cuatrimestre pasado“

La gestión de identidad con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

- “¡Hola! Soy María” (*Identidad*)
- “y aquí están mi usuario y clave para demostrarlo”
  (Verificar la identidad = Autenticar = *AuthN*)
- ”Quiero entregar unos trabajos“
  (Autorizar = *AuthR*:
  Permitir a María usar los servicios
  a los que tiene derecho)
- ”Ya puestos me gustaría cambiarle a Juan la nota
  de Física del cuatrimestre pasado“
  (Autorizar: Evitar que haga cosas que no debe)

Criptografía

definiciones

Criptografía
definiciones

Criptografía *(κριπτοσ γραφοσ)*

Criptografía

definiciones

Criptografía *($\kappa\rho\iota\pi\tau\circ\sigma\ \gamma\rho\alpha\phi\circ\sigma$)*

> *Ciencia de alterar la apariencia de los datos en un esfuerzo por mantenerlos seguros*

Criptografía

definiciones

Texto claro Información que se desea proteger

Texto cifrado Información no inteligible

Clave Mapa que transforma el texto claro en el cifrado. De su tamaño depende la fortaleza del proceso

Criptografía

definiciones

Algoritmo criptográfico Función matemática usada para cifrar y descifrar

Esquema de cifrado Cómo combinar texto, clave y algoritmo

Función de dispersión Obtiene la huella del texto claro

Una vía

irreversible

Una vía

irreversible

No es posible obtener el texto claro a partir del cifrado

```
$1$Bq28UJBA$1wY39esME6PIXGCdzNqg4.
```

Simétrica

un secreto entre dos

Emisor y receptor conocen la clave

Simétrica

un secreto entre dos

Emisor y receptor conocen la clave

- Texto claro + clave = texto cifrado

Simétrica

un secreto entre dos

Emisor y receptor conocen la clave

- Texto claro $+$ clave $=$ texto cifrado
- Texto cifrado $+$ clave $=$ texto claro

Simétrica

un secreto entre dos

Es el método más antiguo,
ya lo usaban los judíos y Julio César

```
Inln phragb rfgb qry pvsenqb
```

Simétrica

un secreto entre dos

Es el método más antiguo,
ya lo usaban los judíos y Julio César

```
ABCDEFGHIJKLMNOPQRSTUVXYZ
NOPQRSTUVWXYZABCDEFGHIKLM

Inln phragb rfgb qry pvsenqb
Vaya cuento esto del cifrado
```

Simétrica

un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

```
Qnonyr neebm n yn mbeen ry nonq
```

Simétrica

un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

`Qnonyrneebmnynmbeenrynonq`

Simétrica

un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

`Qnonyr neebm n yn mbeen ry nonq`

Simétrica

un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

`Qnonyr neebm n yn mbeen ry nonq`

`Qeoeyr eeebm e ye mbeee ry eoeq`

Simétrica

un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

`Qnonyr neebm n yn mbeen ry nonq`

`Qaoayr aeebm a ya mbeea ry aoaq`

Simétrica

un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

`Qnonyr neebm n yn mbeen ry nonq`

`Qaoayr arrbm a ya mbrra ry aoaq`

Simétrica

un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

`Qnonyr neebm n yn mbeen ry nonq`

`Qaoalr arrbm a la mbrra rl aoaq`

Simétrica

un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

`Qnonyr neebm n yn mbeen ry nonq`

`Qaoale arrbm a la mbrra el aoaq`

Simétrica

un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

```
Qnonyr neebm n yn mbeen ry nonq

Qaoale arrbm a la mbrra el aoaq
Dabale arroz a la zorra el abad
```

Asimétrica

un secreto escondido y un secreto a voces

Conocida como criptografía de clave pública

Asimétrica

un secreto escondido y un secreto a voces

Conocida como criptografía de clave pública

Clave pública Algo que debe ser muy conocido

Clave privada Lo que se debe proteger a toda costa

Asimétrica

un secreto escondido y un secreto a voces

Conocida como criptografía de clave pública

Clave pública Para que me puedan enviar mensajes cifrados

Clave privada Para descifrar lo que me envían

Asimétrica

un secreto escondido y un secreto a voces

Conocida como criptografía de clave pública

Clave pública Para que verifiquen lo que envío

Clave privada Para asegurar que lo envío yo

Mantengamos nuestra identidad

yo soy siempre yo

Mantengamos nuestra identidad

yo soy siempre yo

La Gestión de Identidad Federada

Mantengamos nuestra identidad

yo soy siempre yo

La Gestión de Identidad Federada

- Se basa en la infraestructura de Gestión de Identidad de una o más organizaciones

Mantengamos nuestra identidad

yo soy siempre yo

La Gestión de Identidad Federada

- Se basa en la infraestructura de Gestión de Identidad de una o más organizaciones
- Para autenticar y pasar información relativa a la autorización a los proveedores de servicios o los servidores recursos

Mantengamos nuestra identidad

yo soy siempre yo

La Gestión de Identidad Federada

- Se basa en la infraestructura de Gestión de Identidad de una o más organizaciones
- Para autenticar y pasar información relativa a la autorización a los proveedores de servicios o los servidores recursos
- Por medio de acuerdos inter-institucionales

Mantengamos nuestra identidad

yo soy siempre yo

La Gestión de Identidad Federada

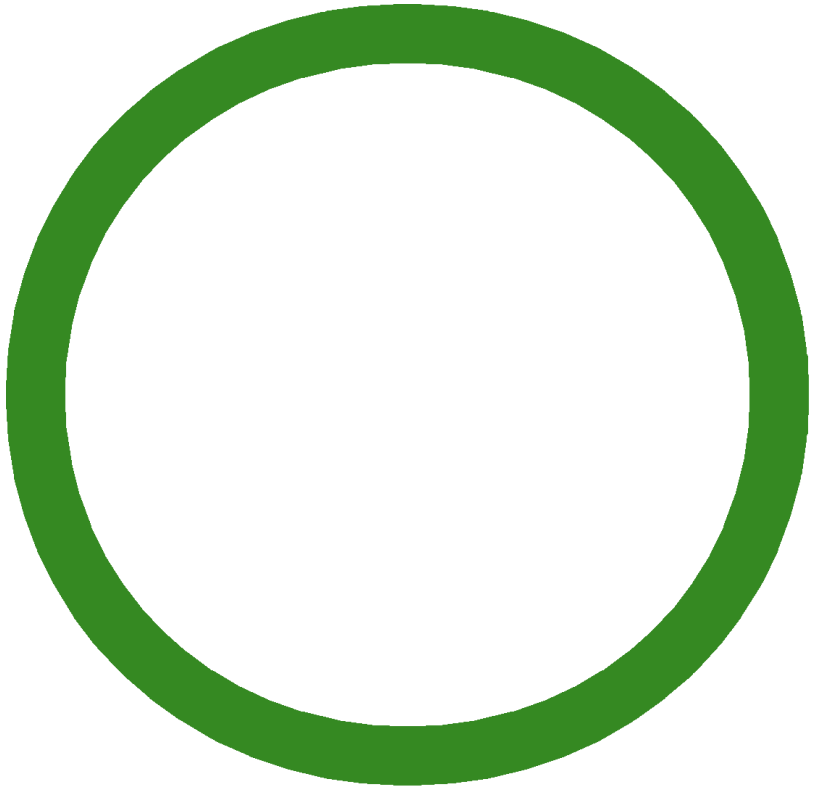
- Se basa en la infraestructura de Gestión de Identidad de una o más organizaciones
- Para autenticar y pasar información relativa a la autorización a los proveedores de servicios o los servidores recursos
- Por medio de acuerdos inter-institucionales
- Facilitados por la pertenencia a una federación

Federación

¿Qué es una federación?

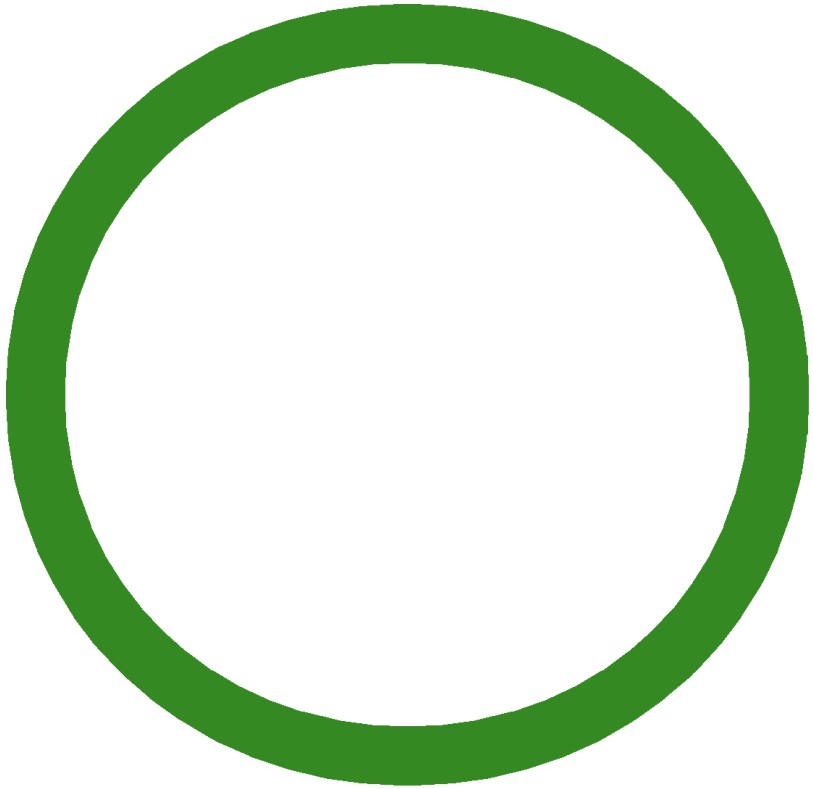
Federación

¿Qué es una federación?



Federación

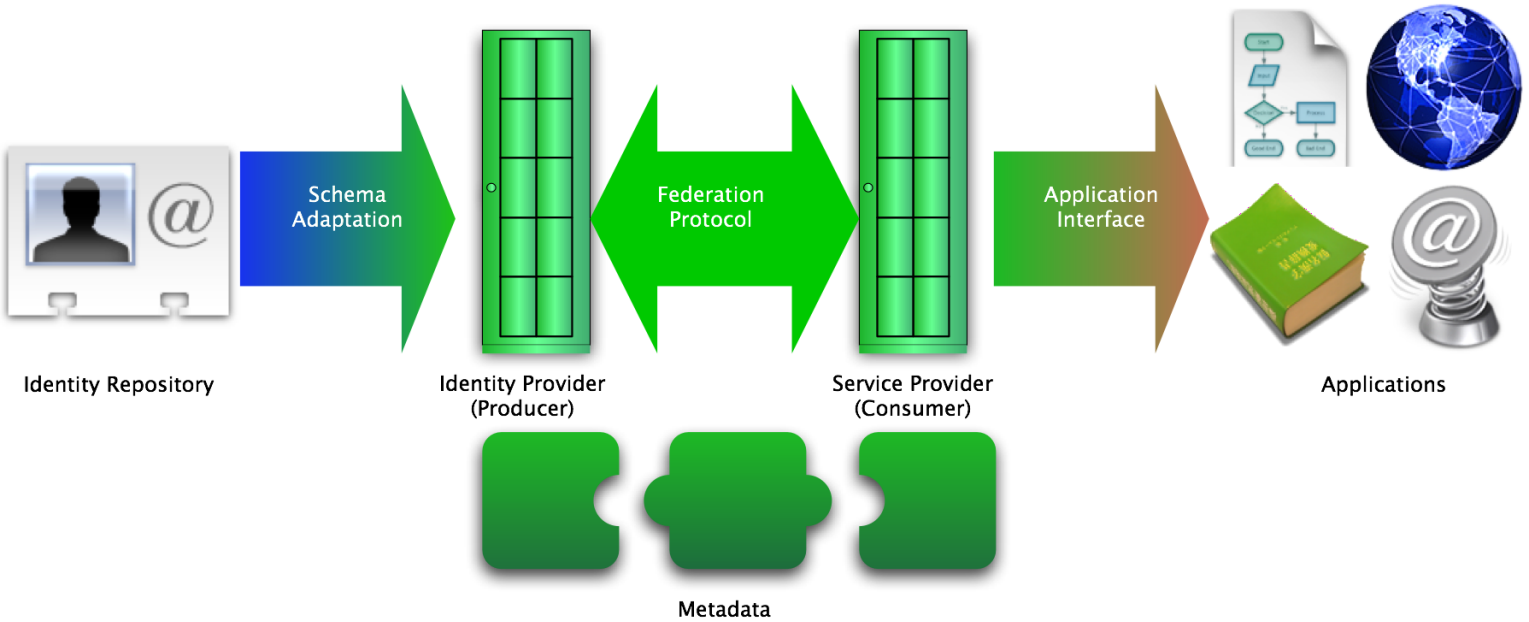
¿Qué es una federación?



de confianza

Federación

¿Qué es una federación?



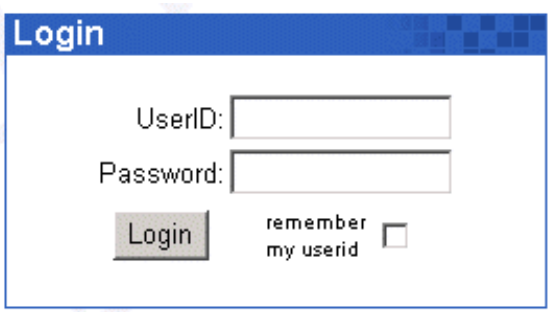
Un caso de éxito

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

Atributo

información sobre la persona

Atributo

información sobre la persona

Ejemplos de atributos

- Los apellidos
- El nombre de pila
- Un número de teléfono
- una dirección de correo

Privacidad

definiciones

del inglés *privacy*

1. *el estado o condición de estar libre de ser observado o molestado por otras personas*
2. *el estado de estar libre de la atención pública*

New Oxford American English Dictionary

Privacidad

definiciones

Privacidad

> *Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*

Diccionario de la Real Academia Española

Privacidad y criptografía

proteger el mensaje

Gracias a la criptografia garantizamos el remitente

Firmo con mi clave privada Solo *yo* he podido firmar

Verifican con mi clave pública *Todos* pueden comprobarlo

Privacidad y criptografía

proteger el mensaje

Gracias a la criptografia garantizamos el destinatario y protegemos el contenido

Cifran con mi clave pública Solo *yo* podré leerlo

Descifro con mi clave privada *Nadie* puede *abirlo*

Privacidad y federación

proteger la persona

La federación permite proteger identidad y los datos personales

- Podemos ser anónimos
- El IdP controla la información personal
- Conocemos que información se envía
- Podemos decidir no enviar datos

Gracias

¿Preguntas?

no se garantizan las respuestas