



Identificación en la USC

Identificación federada mediante SIR/STORK



18.11.2010

Diego Conde Pérez

Índice

- Situación inicial y problemática
- Servicio de identificación centralizado
- Identificación en las aplicaciones
- Identificación mediante usuario/clave y mediante certificado X.509
- Proveedor de identidad para SIR
- Identificación mediante SIR
- Identificación mediante STORK
- Conclusiones y líneas futuras

Situación inicial

- Sistema de provisión de identidades
- Repositorio centralizado
- Identificación en las aplicaciones

Problemática

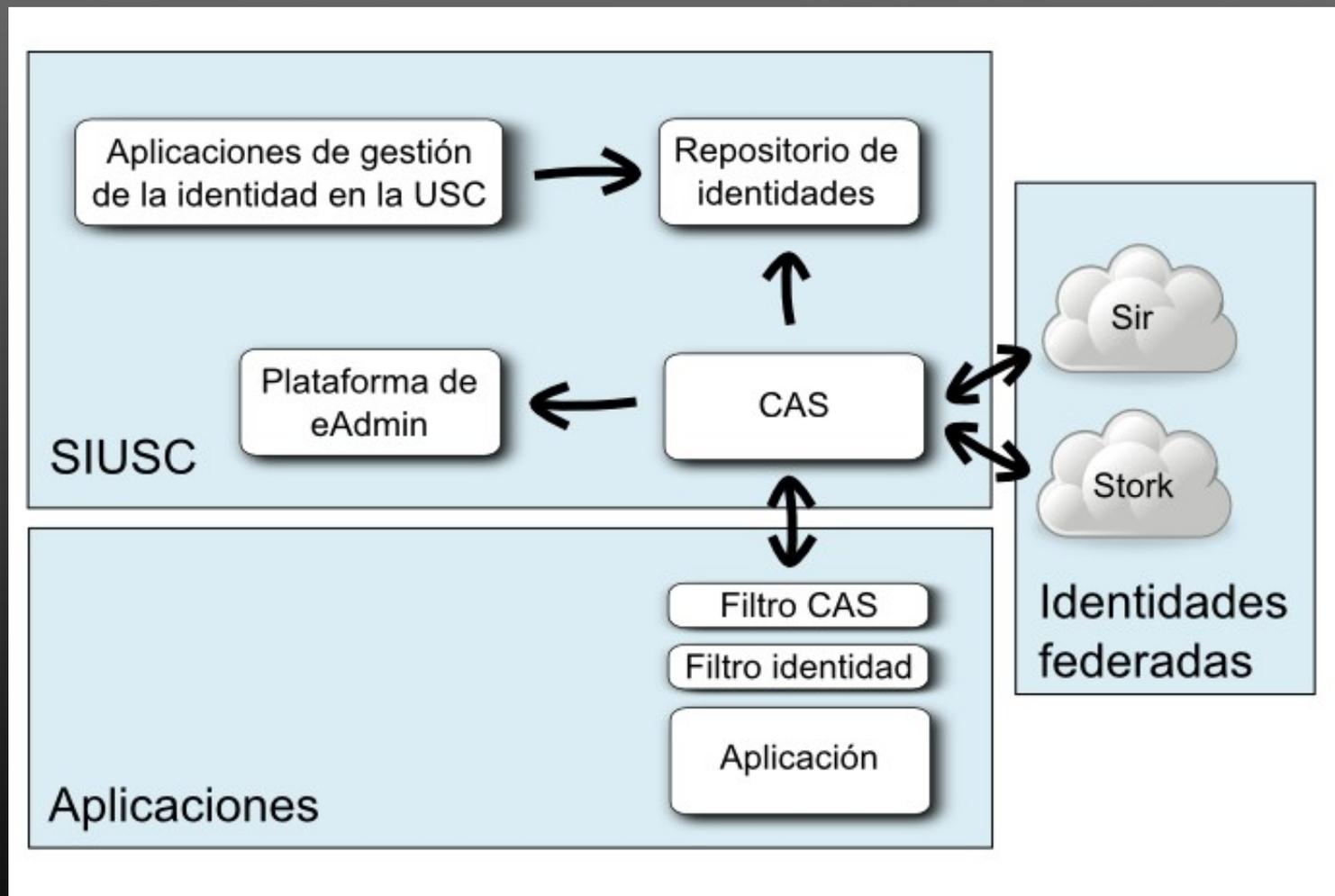
- Dificultades para acometer cambios en:
 - La identificación en aplicaciones
 - El repositorio centralizado
- Imposibilidad de incorporar nuevos sistemas de identificación
- Single Sign On
- Proceso de identificación diferente en función de la aplicación

Servicio de identificación centralizado (SIUSC)

- Solución a la problemática presentada
- Servidor de identificación: Jasig CAS
 - Simple
 - Extensible
 - Experiencia en tecnologías utilizadas
 - Soporte para diversos clientes

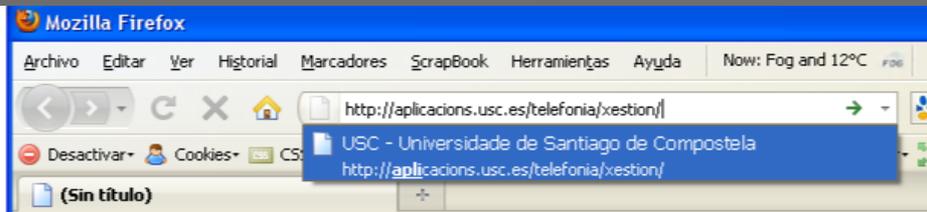
www.jasig.org/cas

Servicio de identificación centralizado (SIUSC)



CAS – Proceso de identificación

- A través de redirecciones HTTP
- Las aplicaciones no tienen acceso a las credenciales
- SSO transparente para el usuario
- La información de identidad puede complementarse con atributos



1 →
HTTP/1.1 302 Movido temporalmente
Date: Fri, 12 Nov 2010 13:08:52 GMT
Server: Apache-Coyote/1.1
Location:
https://www.usc.es/cas/login?service=http%3A%2F%2Faplicac



2



Servizo de identificación centralizado da USC

Área de Tecnoloxías da Información e a Comunicación (ATIC)

[Versión en galego](#) | [Versión en español](#) | [English version](#)

Identificación de usuarios/as

O acceso a esta aplicación está restrinxido aos/as usuarios/as autorizados/as. Se vostede está autorizado/a para utilizar a aplicación debe introducir as súas credenciais.

Se vostede está autorizado/a para acceder a esta aplicación pero non consegue identificarse, consulte a [información dispoñible sobre identificación na USC](#) ou póngase en contacto co [Centro de Atención a Usuarios da USC](#).

Credenciais da USC

Nome de usuario/a:

nome.apellido@usc.es ou nome.apellido@rai.usc.es

Contrasinal:

Avisarme antes de abrir unha sesión noutras aplicacións

Identificación de usuarios/as

O acceso a esta aplicación está restrinxido aos/as usuarios/as autorizados/as. Se vostede está autorizado/a para utilizar a aplicación debe introducir as súas credenciais.

Se vostede está autorizado/a para acceder a esta aplicación pero non consegue identificarse, consulte a [información dispoñible sobre identificación na USC](#) ou póñase en contacto co [Centro de Atención a Usuarios da USC](#).

Credenciais da USC

Nome de **usuario/a**:

nome.apellido@usc.es ou nome.apellido@rai.usc.es

Contrasinal:

Avisarme antes de abrir unha sesión noutras aplicacións

3

```
HTTP/1.1 302 Movido temporalmente
Date: Fri, 12 Nov 2010 11:30:33 GMT
Server: Apache-Coyote/1.1
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache, no-store
Location: http://aplicacion.usc.es/j_spring_security_check?ticket=ST-36818-oh54GPWudwmk9vc39HVj-cas
```

4

USC - Configuración xeral da aplicación



Xestión da telefonía
Módulo de datos básicos e facturación

Período 2010 Abril

[Axuda](#) | [Versión en galego](#) | [Versión en español](#)

Período

[Seleccionar período](#)

Unidades

[Procura de unidades](#)

[Nova unidade](#)

Extensións

**BENVIDOS Á SECCIÓN DE FACTURACIÓN
DE TELEFONÍA FIXA DA UNIVERSIDADE
DE SANTIAGO DE COMPOSTELA**

CAS – Servicio de validación de tickets

- Aplicación de gestión de aplicaciones
- Servicio para las aplicaciones
- Atributos asociados

```
<cas:serviceResponse xmlns:cas='http://www.yale.edu/tp/cas'>
  <cas:authenticationSuccess>
    <cas:user>diego.conde@usc.es</cas:user>
    <cas:attributes>
      <cas:employeeID>36156110H</cas:employeeID>
      <cas:userPrincipalName>diego.conde@usc.es</cas:userPrincipalName>
      <cas:cn>Conde Perez Diego</cas:cn>
      <cas:sn>CONDE PEREZ</cas:sn>
      <cas:employeeType>PAS</cas:employeeType>
      <cas:givenName>DIEGO</cas:givenName>
      <cas:mail>diego.conde@usc.es</cas:mail>
      <cas:tipoAutenticacion>Formulario</cas:tipoAutenticacion>
    </cas:attributes>
  </cas:authenticationSuccess>
</cas:serviceResponse>
```

CAS – Mecanismos identificación

- Componentes:
 - Punto de entrada específico en la aplicación web del CAS
 - Credenciales
 - Gestor de identificación
 - Atributos asociados a la identificación
- No existe un sistema de “plugins”

Identificación en las aplicaciones

- Filtro estándar de identificación con el CAS mediante validación de tickets
- Lista de métodos de identificación permitidos en la aplicación
- Mecanismo para forzar la reautenticación
- Configuración en el CAS de aplicaciones y métodos de

Credenciales CAS: usuario y clave

- Identidad gestionada por la USC
- Método de identificación por defecto
- Repositorio de identidades centralizado
- Atributos entregados a las aplicaciones:
 - Identificador usuario
 - Nombre, apellidos, NIF, mail
 - Tipo de usuario

Credenciales CAS: certificado X.509

- Identidad no gestionada por la USC
- Validación de certificados mediante plataforma de administración electrónica
- Atributos entregados a las aplicaciones:
 - Se añaden los mismos que con usuario/clave si el usuario tiene identidad en la USC
 - Datos incluidos en el certificado en estructura normalizada

SIR

- Proyecto de RedIRIS
- Identidad federada para comunidad universitaria española
- Dos papeles
 - Proveedor de identidad
 - Proveedor de servicio

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

USC como proveedora de identidad en SIR

- Conector PAPI para el sistema local de identidad
- CAS no dispone de conector PAPI
- Pasarela PAPI-CAS: icGPoA
- Identificación mediante CAS

USC como proveedora de servicios en SIR

- Dos opciones de integración:
 - Aplicación por aplicación
 - En el sistema de identificación centralizado
- Desarrollo de un nuevo sistema de identificación para el CAS

Credenciales CAS: SIR

- Proceso de identificación en SIR
- Comunicación entre CAS y SIR mediante PAPI
- Punto de partida: filtro SIR en Java de RedIRIS
- Se comunican a las aplicaciones los atributos recibidos (como mínimo uid y sho).

Identificación de usuarios/as

O acceso a esta aplicación está restrinxido aos/as usuarios/as autorizados/as. Se vostede está autorizado/a para utilizar a aplicación debe introducir as súas credenciais.

Se vostede está autorizado/a para acceder a esta aplicación pero non consegue identificarse, consulte a información dispoñible sobre identificación na USC ou pónhase en contacto co [Centro de Atención a Usuarios da USC](#).

Credenciais da USC

Nome de usuario/a:

nome.apellido@usc.es ou
nome.apellido@rai.usc.es

Contraseñal:

Avisarme antes de abrir unha sesión noutras aplicacións

Identificarse

Outros métodos de identificación



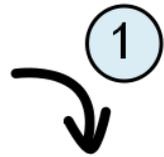
Proyecto Stark

Para cidadáns de países da UE con credenciais admitidas no Proyecto Stark.



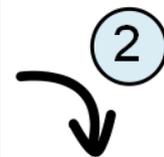
Servizo de Identidade de RedIRIS (SIR)

Para PDI, PAS e alumnos de universidades españolas integradas no Servizo de Identidade de RedIRIS (SIR).



Servicio de Identidad digital - RedIRIS

Buscar por comunidad autónoma



- B.C.B.L.
- B.O.E.
- BSC-CNS
- Biblioteca de Catalunya
- C.E.S.G.A.
- C.I.C.A.
- C.N.I.O.
- CIEMAT
- CSIC

USC - Configuración xeral da aplicación



Xestión da telefonía

Módulo de datos básicos e facturación

Período 2010 Abril

[Axuda](#) | [Versión en galego](#) | [Versión en español](#)

Período

Seleccionar período

Unidades

Procura de unidades

Nova unidade

Extensións

BENVIDOS Á SECCIÓN DE FACTURACIÓN

DE TELEFONÍA FIXA DA UNIVERSIDADE

DE SANTIAGO DE COMPOSTELA

STORK

- Proyecto europeo
- Sistemas de identificación electrónica nacionales de cada estado miembro
- Interconexión a través de RedIRIS
- Integración en el sistema de identificación técnicamente muy similar a SIR

<https://www.eid-stork.eu/>

Credenciales CAS: STORK

- Proceso de identificación en STORK
- Comunicación entre CAS y STORK mediante PAPI a través de RedIRIS
- Base de código idéntica a la de SIR
- Atributos varían en función del país en el que se realiza la identificación

Identificación de usuarios/as

O acceso a esta aplicación está restrinxido aos/as usuarios/as autorizados/as. Se vostede está autorizado/a para utilizar a aplicación debe introducir as súas credenciais.

Se vostede está autorizado/a para acceder a esta aplicación pero non consegue identificarse, consulte a [información dispoñible sobre identificación na USC](#) ou póñase en contacto co [Centro de Atención a Usuarios da USC](#).

Credenciais da USC

Nome de usuario/a:

nome.apellido@usc.es ou
nome.apellido@rai.usc.es

Contraseñal:

Avisarme antes de abrir unha sesión noutras aplicacións

Identificarse

Outros métodos de identificación



Proxecto Stork

Para cidadáns de países da UE con credenciais admitidas no Proxecto Stork.



Servizo de Identidade de RedIRIS (SIR)

Para PDI, PAS e alumnos de universidades españolas integradas no Servizo de Identidade de RedIRIS (SIR).



Italia

Österreich

Portugal

1



Pasarela piloto STORK - RedIRIS

Seleccionar en un mapa



2



USC - Configuración xeral da aplicación



Xestión da telefonía

Módulo de datos básicos e facturación

Período 2010 Abril

[Axuda](#) | [Versión en galego](#) | [Versión en español](#)

Período

[Seleccionar período](#)

Unidades

[Procura de unidades](#)

[Nova unidade](#)

[Extensións](#)

BENVIDOS Á SECCIÓN DE FACTURACIÓN

DE TELEFONÍA FIXA DA UNIVERSIDADE

DE SANTIAGO DE COMPOSTELA

Conclusiones

- Proceso de identificación transparente para las aplicaciones
- Incorporación “sencilla” de nuevos mecanismos de identificación
- Complejidad adicional en las aplicaciones:
 - Mecanismos de identificación permitidos
 - Reautenticación
 - Diversidad de atributos en función del mecanismo de identificación

Líneas futuras

- Liberación del código en forja de RedIRIS
- Difusión de sistemas de identificación estándar entre proveedores
- Marco legal para la confianza en las identidades generadas en SIR
- Conjunto de atributos mínimo para intercambio de identidades entre universidades
- Localización de SIR

Muchas gracias

Universidade de Santiago de Compostela

Diego Conde Pérez

José Manuel Piñeiro Domínguez

Xosé Antonio Rubal López

diego.conde@usc.es

josemanuel.pineiro@usc.es

xoseantonio.rubal@usc.es