Federación de identidades y servicios sobre SIR: el Campus MareNostrum.

RedIRIS

Valladolid

1 de diciembre de 2011

José Juan Sánchez Manzanares <pepe.manzanares@si.upct.es>
Francisco Yepes Candel <pacoy@um.es>
Juan Carlos Giménez Moncada <moncada@um.es>
Antonio Máximo González Adán <antonio.gonzalez@si.upct.es>

Índice

1.- ¿Qué es el Campus Mare Nostrum?

1. ¿Qué es el Campus Mare Nostrum?

http://www.campusmarenostrum.es/

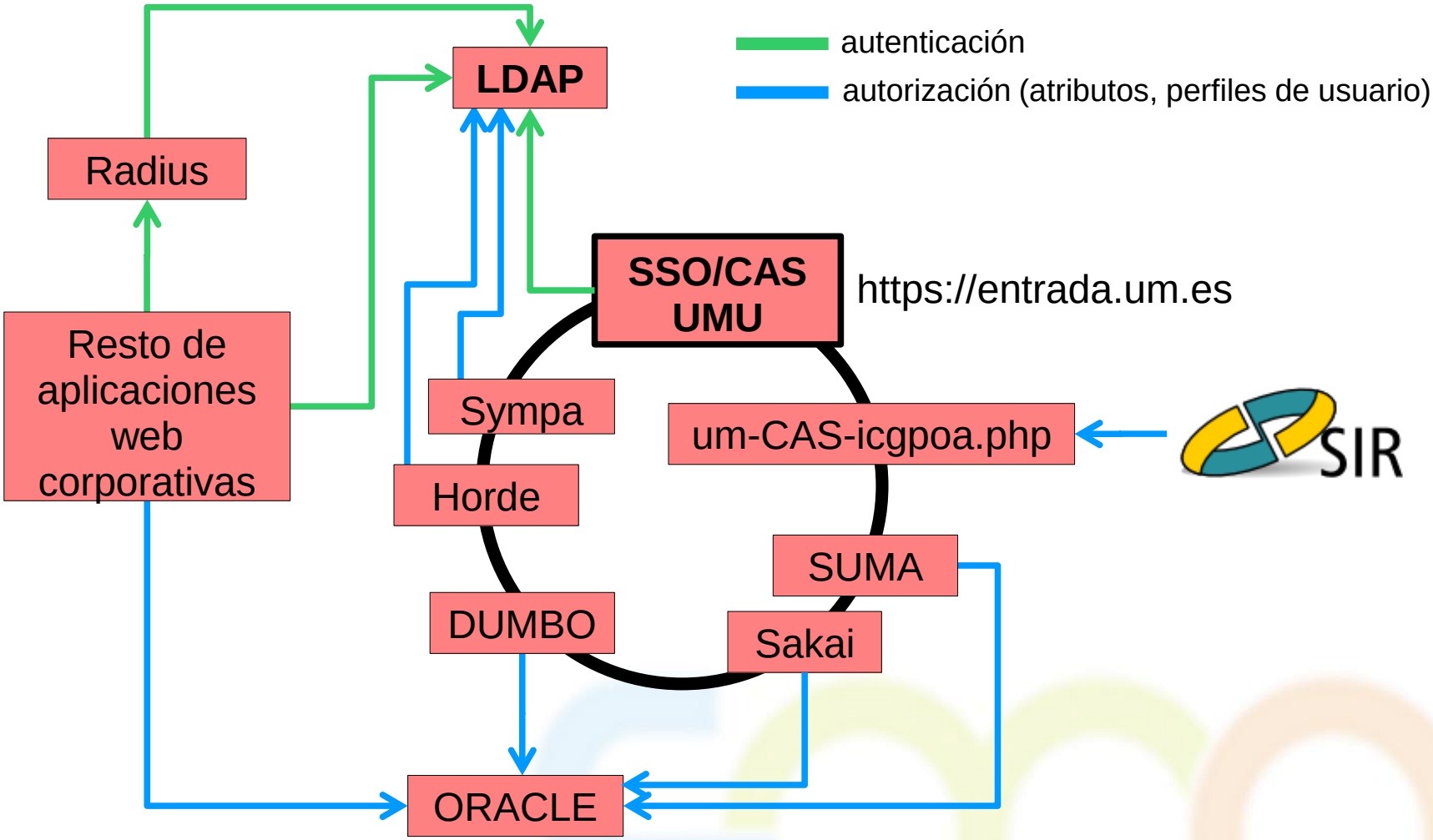
"**Campus Mare Nostrum 37/38** es el Campus de Excelencia Internacional de la Universidad de Murcia y la Universidad Politécnica de Cartagena que, junto a centros de investigación, administraciones públicas, organizaciones internacionales, parques tecnológicos y empresas, persigue transformar la Región de Murcia en un foco de excelencia educativa, científica, productiva y cultural por y para el Mediterráneo."

2.- Situación de Partida

Universidad de Murcia (enero 2011)

- Proveedor de identidad (**IdP)** de **SIR** desde julio de 2009.
- No proveedores de servicio (**SP)** en **SIR.**
- Un **SSO** (**CAS**) en producción desde enero de 2010.
- Aplicaciones web corporativas autentican contra **Open LDAP**:
  - Las más importantes integradas en el SSO (CAS).
  - Resto autentican directamente contra LDAP o RADIUS.
  - Atributos de usuario (perfiles) en Open LDAP y BBDD ORACLE.

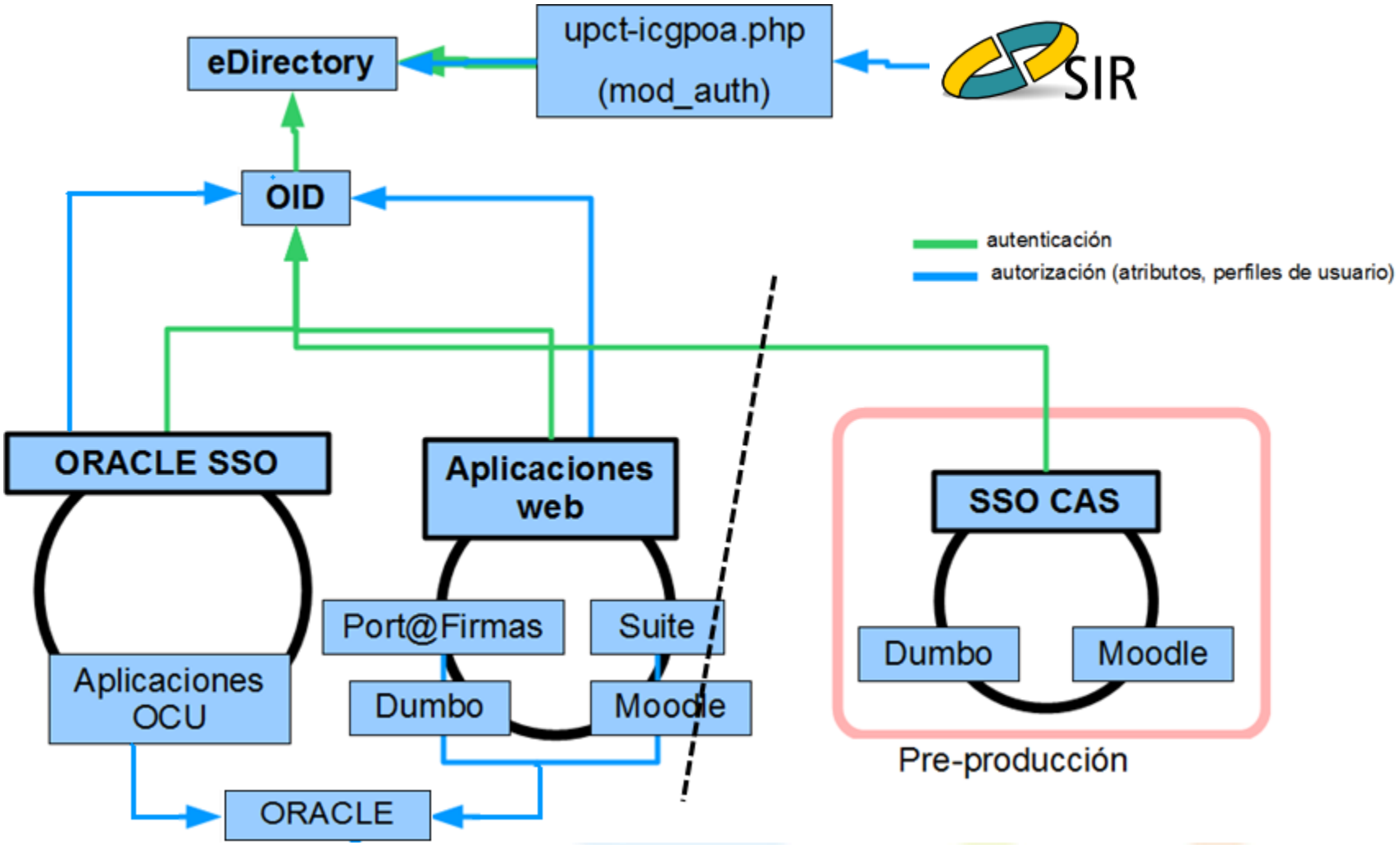
Universidad de Murcia (enero 2011)



Universidad Politécnica de Cartagena (enero 2011)

- IdP de SIR desde enero de 2010. No es **SP** en **SIR.**
- Se usan dos directorios red
  - El directorio OID de Oracle (junto con su SSO) se usa para autenticación y autorización (perfiles) en aplicaciones de OCU.
    - SSO de Oracle tiene configurado un plugin o conector para delegar la autenticación de los usuarios en eDirectory.
  - Resto de aplicaciones corporativas se autentican usando el protocolo LDAP contra el OID.
  - Perfiles de Usuario en BBDD y en OID.
- Desplegado CAS de Jasig en **pre-producción.**

Universidad Politécnica de Cartagena (enero 2011)



3.- Requisitos

Los propios de una federación de identidades:

- Que los usuarios (PDI, PAS y alumnos) de una universidad puedan usar sus credenciales de origen para acceder a determinados servicios y aplicaciones de la otra.

- Establecer niveles de acceso en función del perfil (atributos) de los usuarios.

- Mantener separados los servicios de autenticación/autorización propios de cada universidad:
  - ► Repositorios de identidad independiente.
  - ► Sistemas gestión de identidad independientes.

Adicionales

- Simplificar al máximo el proceso de autenticación de los usuarios.

- Simplificar la gestión de perfiles de usuario (evitar, en la medida de lo posible, el mantenimiento de identidades de una organización en la otra).

- **En definitiva**: que el impacto sea mínimo para la organización, para los usuarios y para la administración de los servicios y aplicaciones.

4.- Elección del WAYF (SIR de RedIRIS)

WAYF (Were Are You From?)

- Hub de interconexión de una federación de identidades.
- Permite que usuarios de una organización puedan acceder a servicios de otra.
- Redirige al usuario al sistema de autenticación de su organización de origen (IdP) para que proporcione sus credenciales.
- Recopila atributos del usuario en el IdP para pasárselos al servicio de la organización de destino (SP) para que el SP compruebe si está autorizado a usar el servicio.
- Opcionalmente: filtra atributos, informa y solicita permiso al usuario para transmitirlos al SP.

4. Elección del WAYF (SIR de RedIRIS)

Motivos que nos llevaron a usar la infraestructura de RedIRIS (http://www.rediris.es/sir/):

- SIR probado y funcionando desde hace tiempo.
- Bien documentado y bien soportado.
- **Aprovechar experiencia y "know how".**
- Entornos de desarrollo y producción.
- Protocolo de federación (PAPI v1.0) muy flexible.
- Múltiples protocolos de salida: PAPI, SAML, OpenID, Live@EDU, ...
- Posibilidad de incorporar a la federación CMN SPs ya conectados a SIR.
- **Evitamos despliegue de infraestructura propia.**

5.- Elección del SSO (CAS)

5. Elección del SSO (CAS)

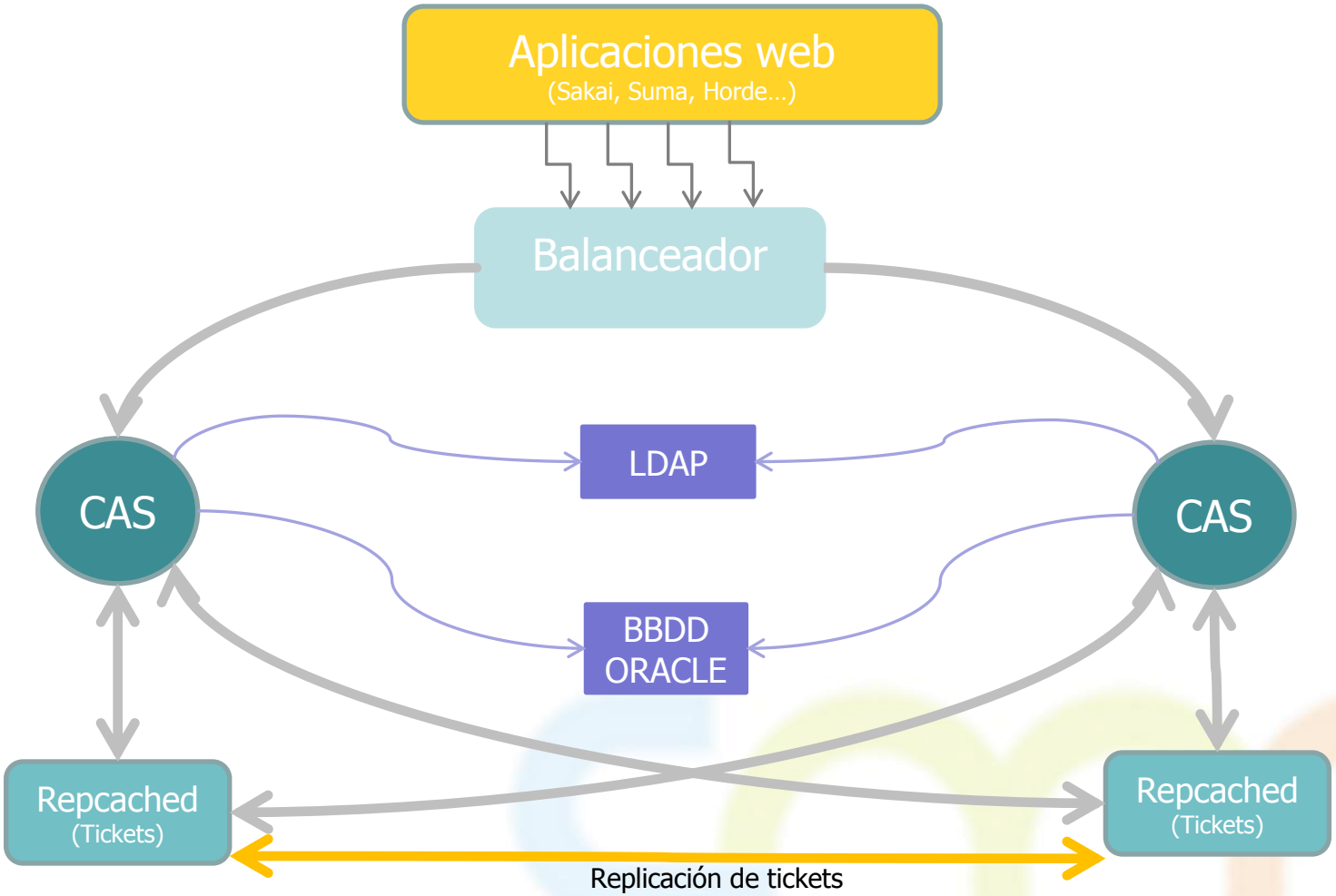
CAS (Central Authenticacion Service) creado originalmente por la Universidad de Yale para crear una manera fiable de autenticar a un usuario en aplicaciones.

- Es **código abierto**. Sin costes.
- Existe una gran comunidad de usuarios y la web aloja gran cantidad de **documentación**.
- Existe una comunidad de desarrolladores de CAS.
- Participan más de 40 universidades en el proyecto.
- Software de terceros incluyen CAS como opción de autenticación (Joomla, Sakai, Moodle, Websphere Portal, Mediawiki, Tomcat, Bonito, Oracle SSO, ...).
- Es **extensible**.

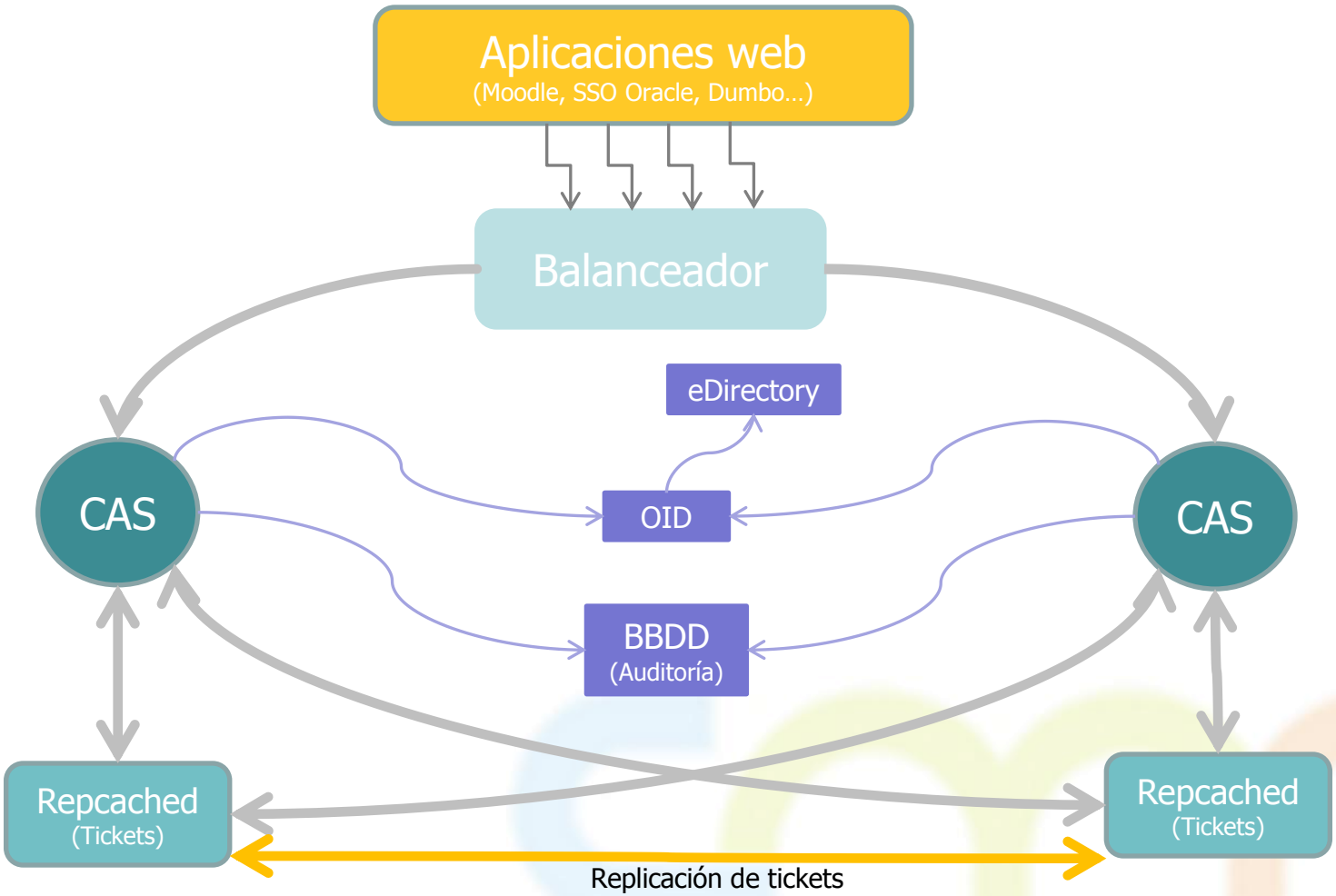
Principales Razones

- Funcionando en la UMU desde enero de 2010 sin problemas.
- En la UPCT lo habíamos evaluado en nuestras aplicaciones corporativas con éxito. Entorno de pre-producción estable.
- Homogeneización de los entornos de desarrollo y producción de la UPCT y la UMU (conocimiento compartido).
- **La USC había desarrollado una extensión para autenticación SIR** (CAS es extensible, lo que permite definir nuevas formas de autenticación).
- **Permite caseizar el SSO de Oracle (requisito de la UPCT).**

Arquitectura del SSO/CAS en la UMU



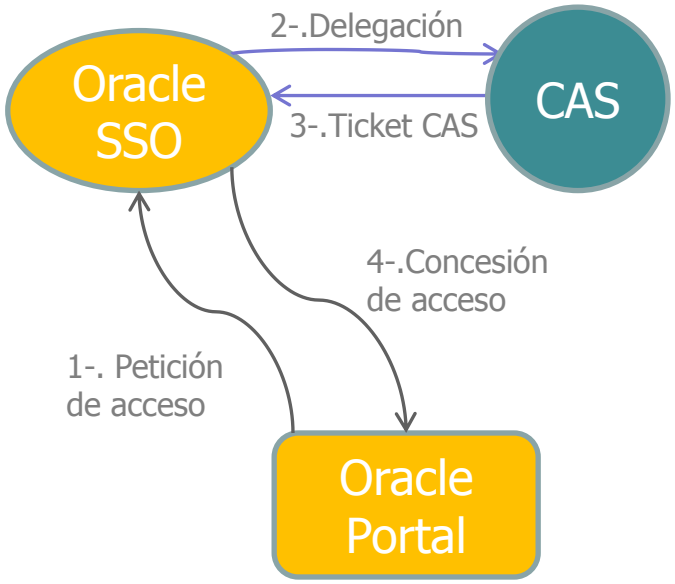
Arquitectura del SSO/CAS en la UPCT



6.- “Caseizando” el SSO de Oracle

En que consiste Caseizar el SSO de Oracle:

1. En aplicar un **filtro CAS** al SSO de Oracle.
2. Sustituir el plugin Oracle SSO por **el plugin CASAuthenticator**.
3. Modificar el proceso de desconexión para salir simultáneamente de CAS y OracleSSO.



En Oracle Portal, los usuarios deben estar dados de alta en OID para poder acceder. La **autorización** en Oracle Portal se basa en pertenencia a grupos LDAP.

Los usuarios serán registrados en el primer acceso.

7.- El Conector CAS-SIR/STORK de la Universidad de Santiago de Compostela

7. El Conector CAS SIR/STORK

Extensión del CAS creada por la **Universidad de Santiago de Compostela** (USC):

- Pasarela PAPI-CAS para el SIR.
- Comunicación entre CAS y SIR mediante protocolo PAPI.
- Instalación sencilla y bien documentada.
- Presentado en las Jornadas Técnicas de Rediris 2010.

La extensión también ofrece soporte para **STORK**, donde se usan los sistemas de identificación electrónica nacionales de cada estado miembro de la UE.

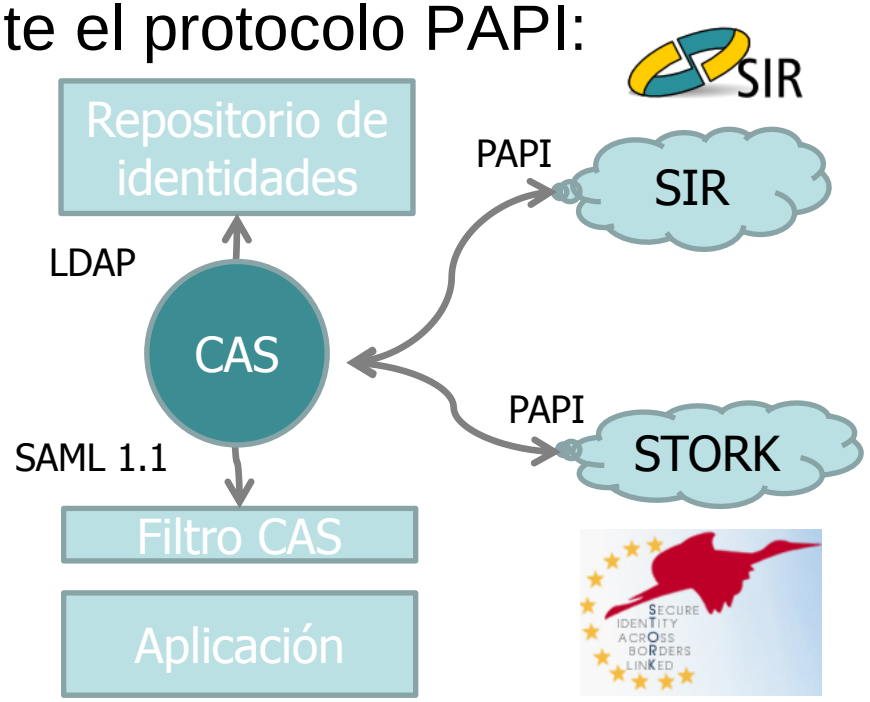
Adicionalmente, la USC ha creado un **filtro de identidad** de aplicaciones (independiente del conector SIR/STORK).

- Niveles de confianza en la autenticación (levels of assurance).

7. El Conector CAS SIR/STORK

- El SIR comunica al CAS los atributos acordados entre las dos universidades mediante el protocolo PAPI:

sPUID	22989092V
mail	pepe.manzanares@si.upct.es
gn	JOSÉ JUAN
sn1	SÁNCHEZ
sn2	MANZANARES
ePA	stuff|faculty
uid	22989092V
sHO	upct.es
…	



- CAS comunica los atributos a las aplicaciones en SAML.
  - Las aplicaciones recogen los atributos haciendo uso de las librerías de CAS.

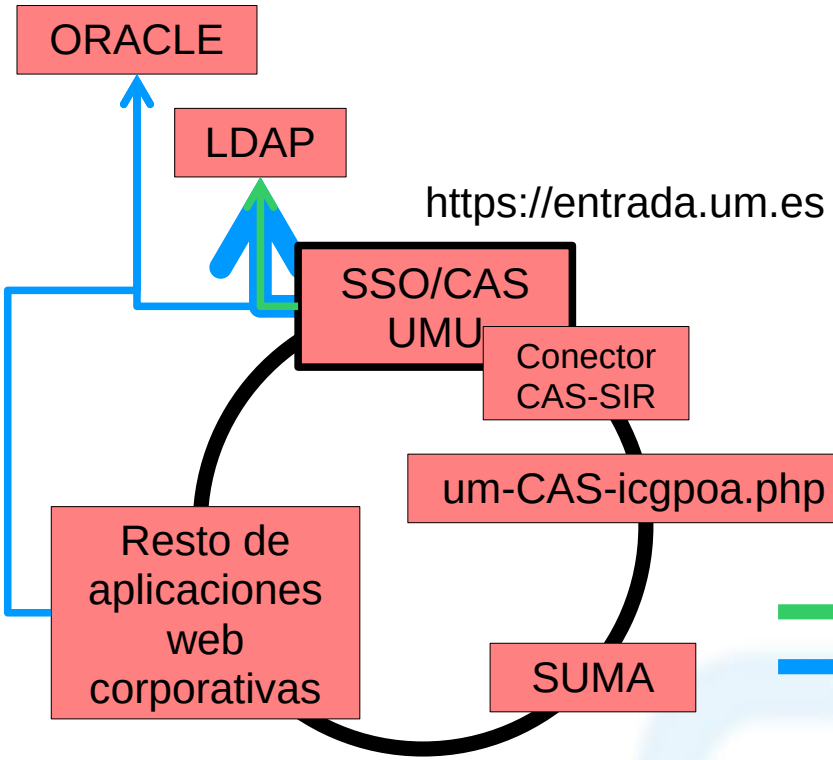
8.- Estado Actual de la Federación CMN

Universidad de Murcia (diciembre 2011)

- La mayor parte de las aplicaciones en el SSO/CAS
- CAS sigue autenticando contra LDAP
- Aplicación de campus virtual (SUMA) primera aplicación federada en CMN[1]
- Añadidas funcionalidades nuevas al conector CAS-SIR: papihli y serviceApp[1]
- Recopilación de perfiles centralizado en CAS a partir de consultas al LDAP y a ORACLE
- Formulario de entrada modificado para contemplar la federación CMN (y STORK)

[1]En entorno de pruebas https://sso.um.es

Universidad de Murcia (noviembre 2011)

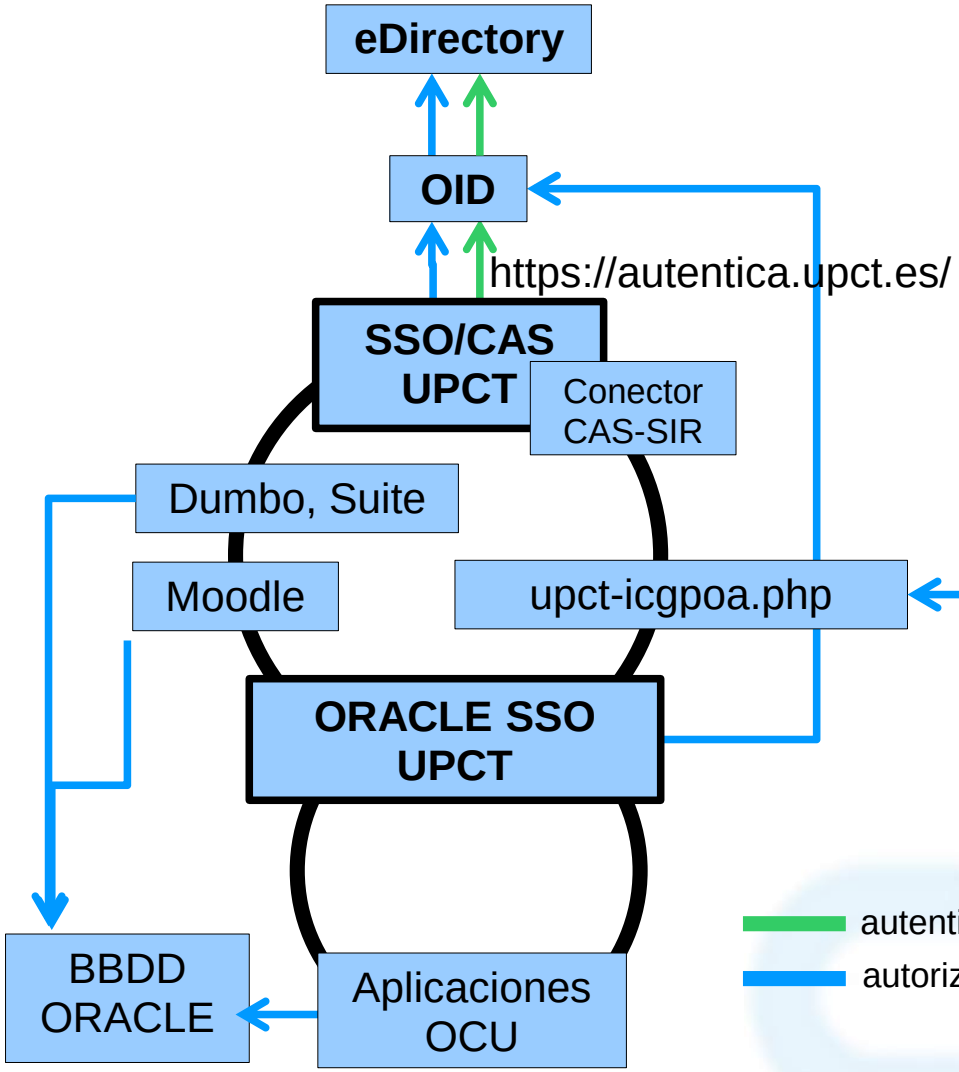


Universidad Politécnica de Cartagena (diciembre 2011)

- Todas las aplicaciones ORACLE en el SSO/CAS vía "caseización" de Oracle SSO.
- Resto de aplicaciones en el SSO/CAS.
- CAS autentica contra OID.
- Portal de Servicios UPCT primera aplicación federada en CMN.
- Formulario de entrada modificado para contemplar la federación CMN (y STORK).

8. Estado actual de la Federación CMN

Universidad Politécnica de Cartagena (noviembre 2011)



SIR

autenticación

autorización (atributos, perfiles de usuario)

Servicios a compartir entre las dos universidades

Gestión Académica y Secretaría Virtual:
- Consulta Calendario Académico
- Consulta Oferta de Cursos de Consejo de Gobierno
- Consulta Tablón de Gestión Académica
- Consulta Titulaciones UMU

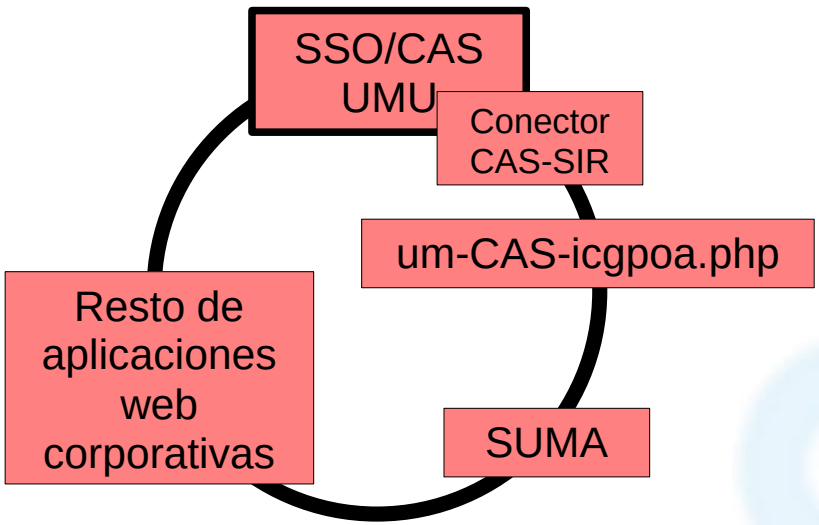
Extracurricular:
- Foros
- Chat
- Reserva de Aula de Libre Acceso (esto permitirá el uso del pc reservado en nuestras ALAS)
- Tablón de Anuncios
- Reserva de Cabinas Bibliotecas
-Ecomóvil
- Deportes: (Reserva de Instalaciones Deportivas, Inscripción en Actividades Deportivas, Cursos y Actividades UMUdeporte, Alta y renovación de Socios UMUdeporte, Reserva de Centro de Medicina Deportiva)

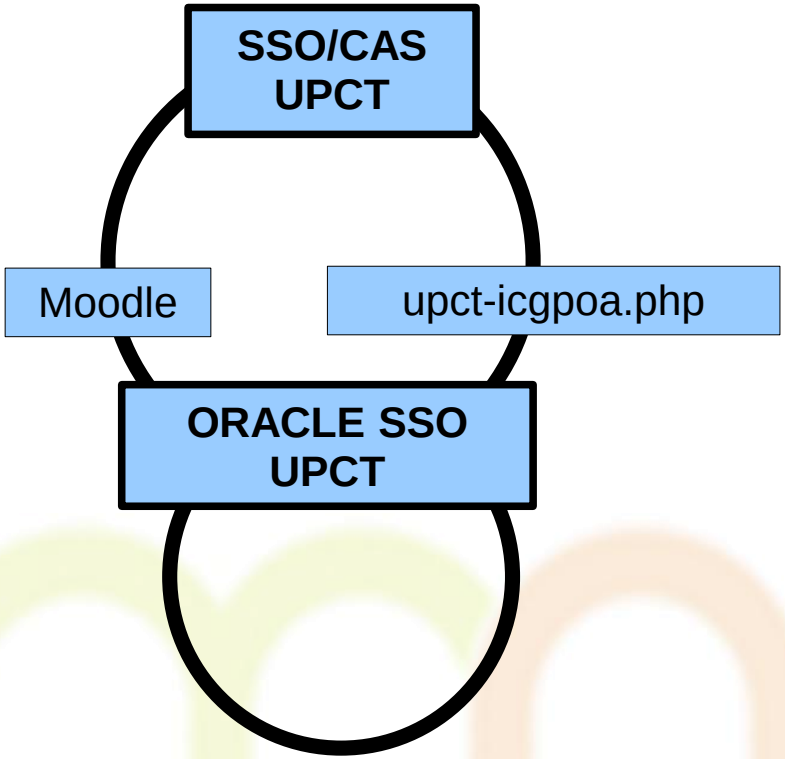
Comercial:
- Publicaciones

BIBLIOTECA UNIVERSITARIA: Servicio de préstamo

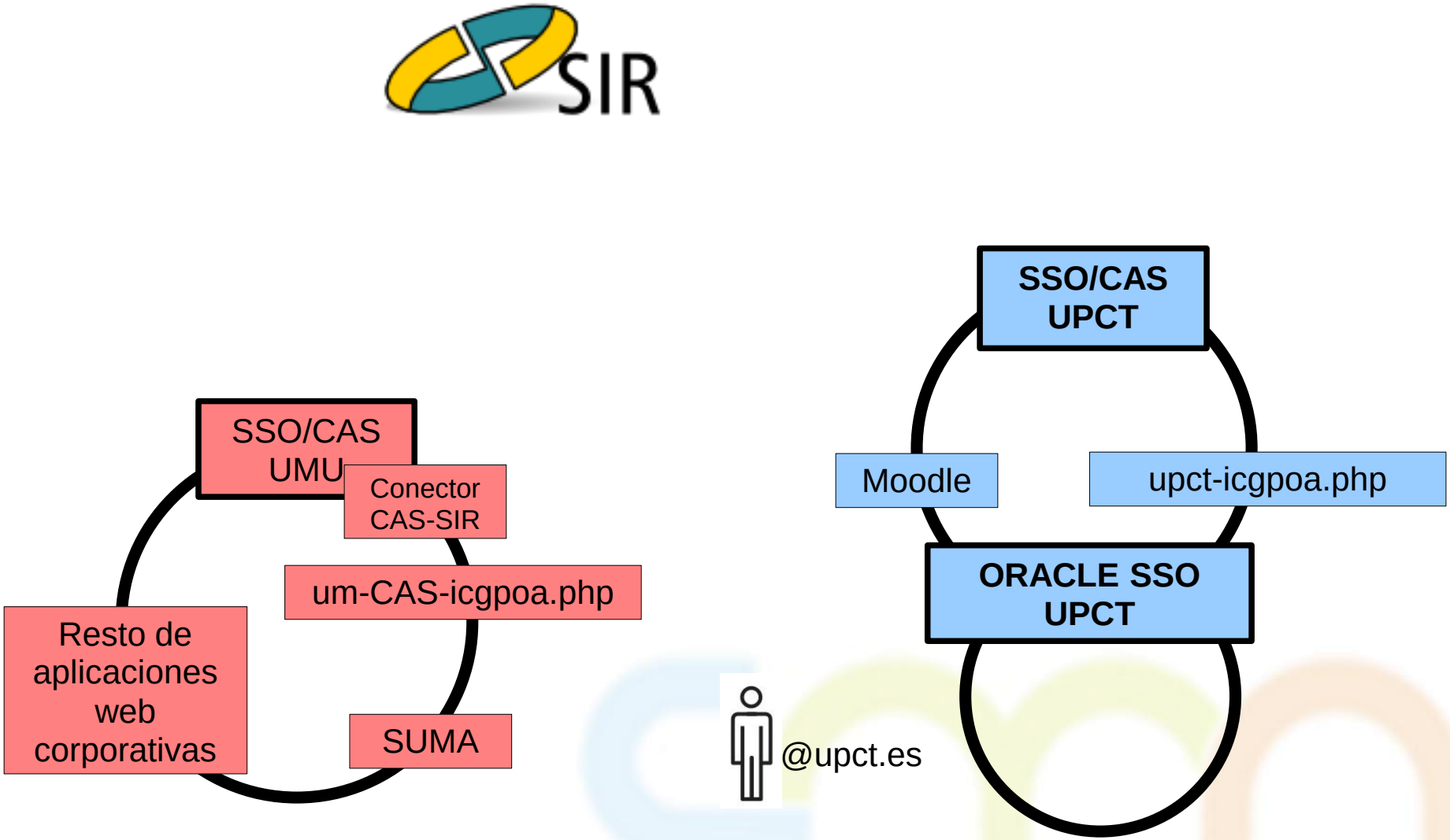
9.- Ejemplo de uso de la Federación CMN

9. Ejemplo de uso de la Federación CMN

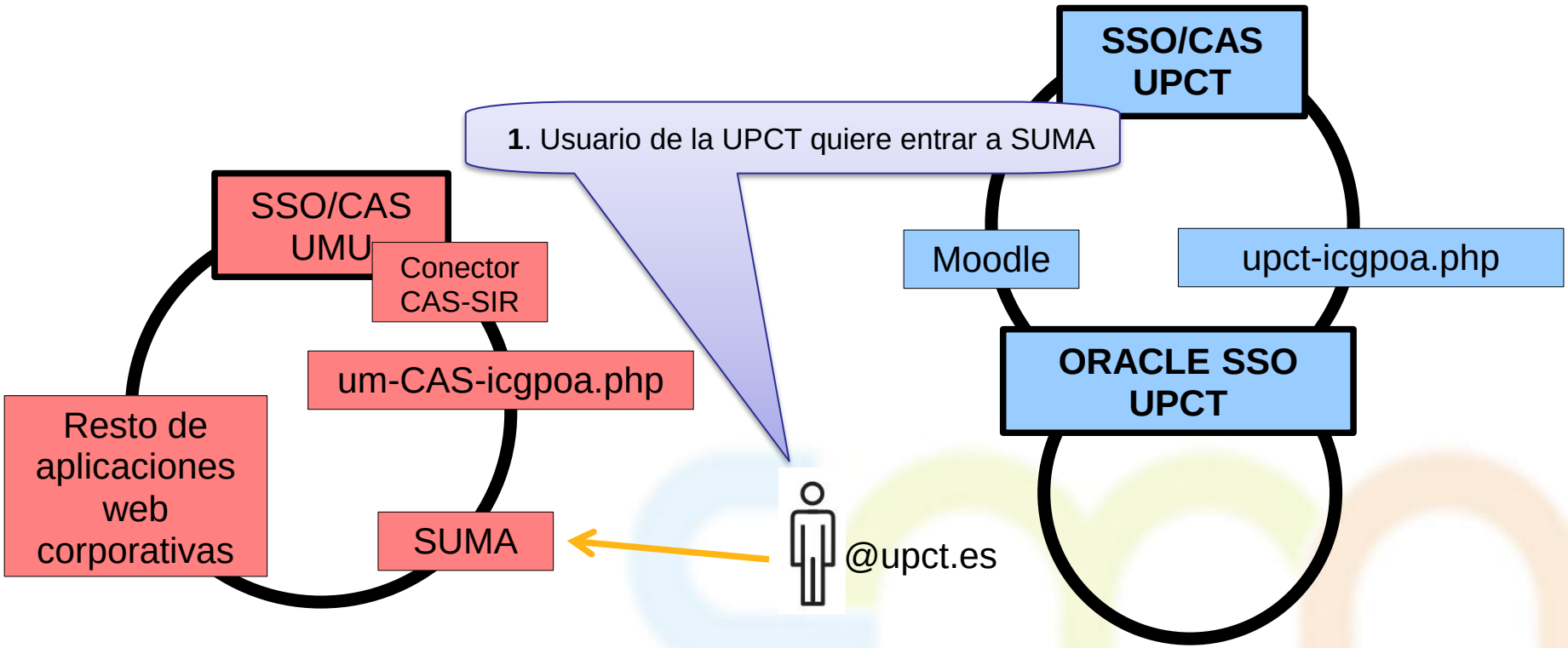




9. Ejemplo de uso de la Federación CMN



9. Ejemplo de uso de la Federación CMN



9. Ejemplo de uso de la Federación CMN

2. Como SUMA está caseizada, redirige al usuario al portal de entrada de la UMU

SSO/CAS UMU

onector CAS-SIR

um-CAS-icgpoa.php

Resto de aplicaciones web corporativas

SUMA

1

@upct.es

SSO/CAS UPCT

Moodle

upct-icgpoa.php

ORACLE SSO UPCT

9. Ejemplo de uso de la Federación CMN

SIR

SSO/CAS UMU

Conector CAS-SIR

um-CAS-icgpoa.php

Resto de aplicaciones web corporativas

SUMA

2

1

@upct.es

3. El usuario pincha en el botón CMN

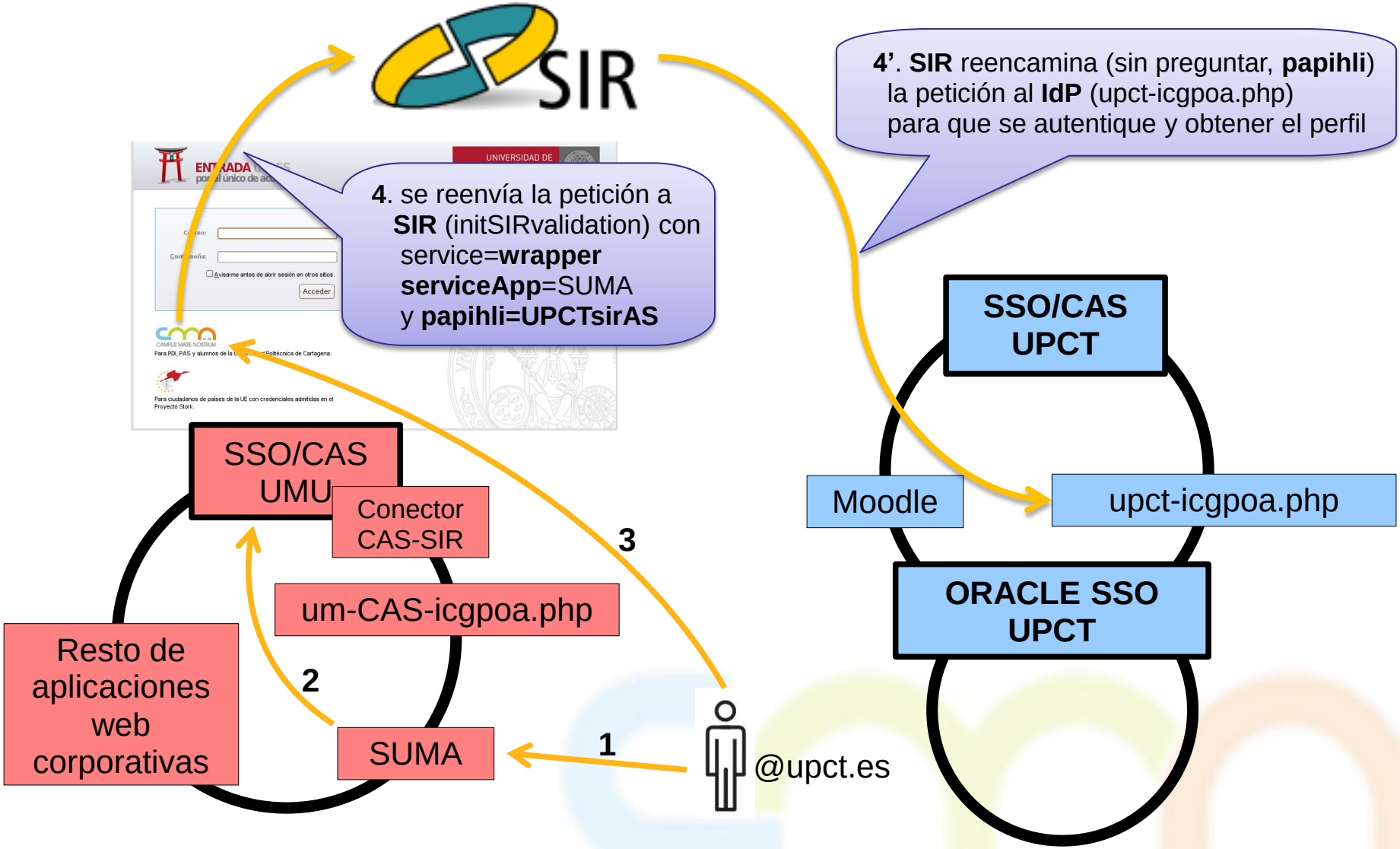
SSO/CAS UPCT

Moodle

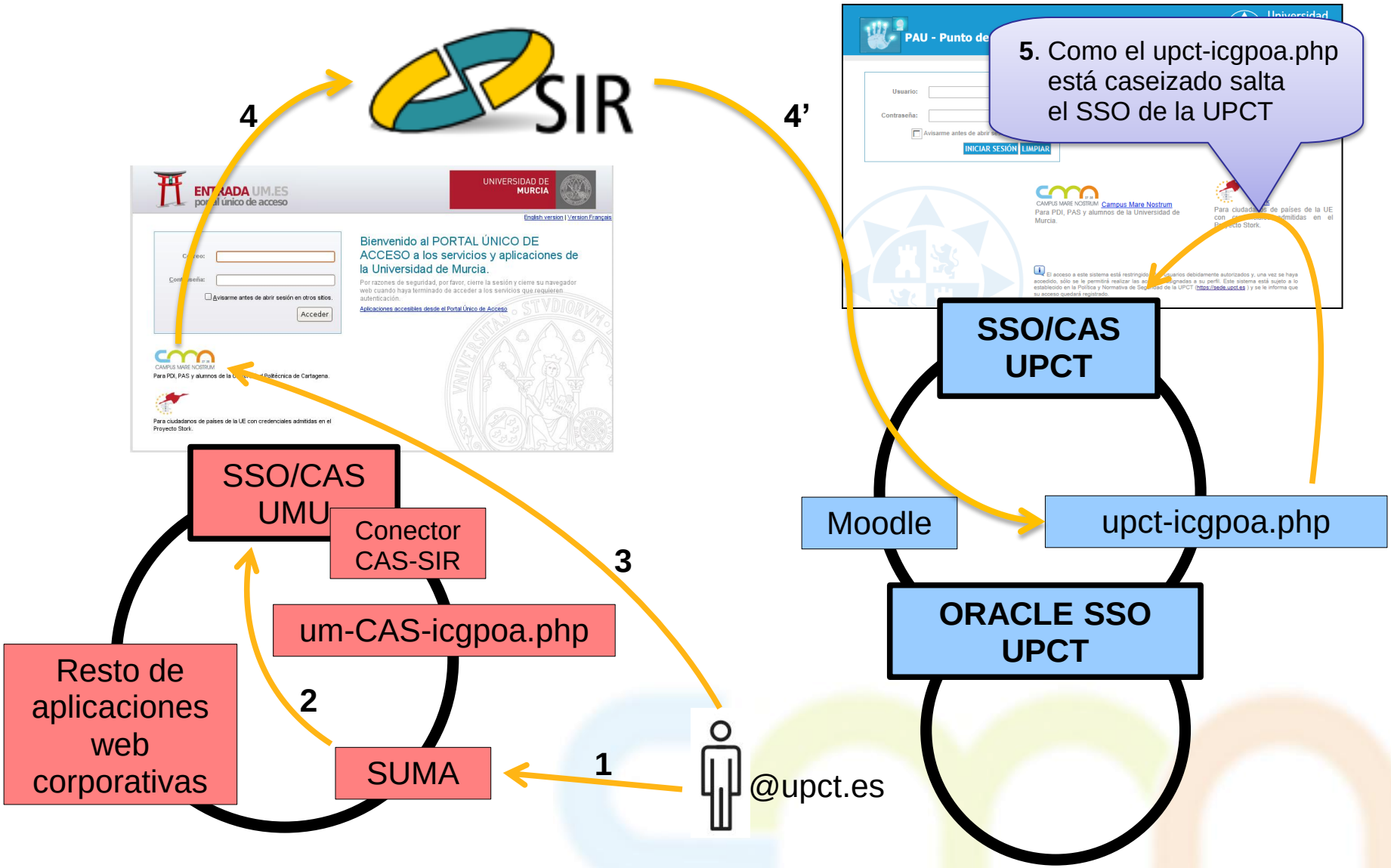
upct-icgpoa.php

ORACLE SSO UPCT

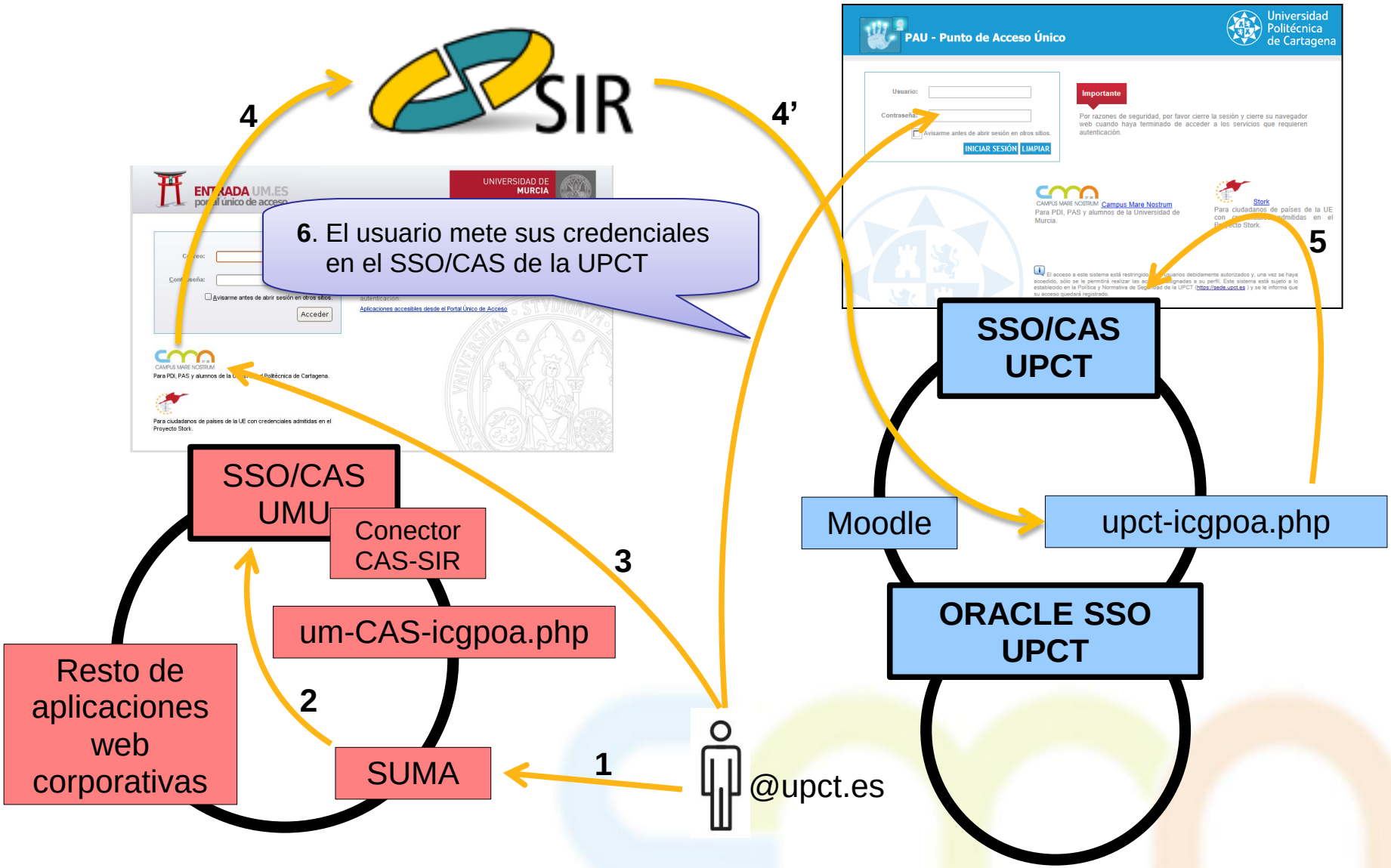
9. Ejemplo de uso de la Federación CMN



9. Ejemplo de uso de la Federación CMN



9. Ejemplo de uso de la Federación CMN



9. Ejemplo de uso de la Federación CMN

7. Si las credenciales son correctas se efectúa la autenticación, se recogen los atributos del usuario y se mandan a SIR

SSO/CAS UMU

Conector CAS-SIR

um-CAS-icgpoa.php

Resto de aplicaciones web corporativas

SUMA

@upct.es

SSO/CAS UPCT

Moodle

upct-icgpoa.php

ORACLE SSO UPCT

1

2

3

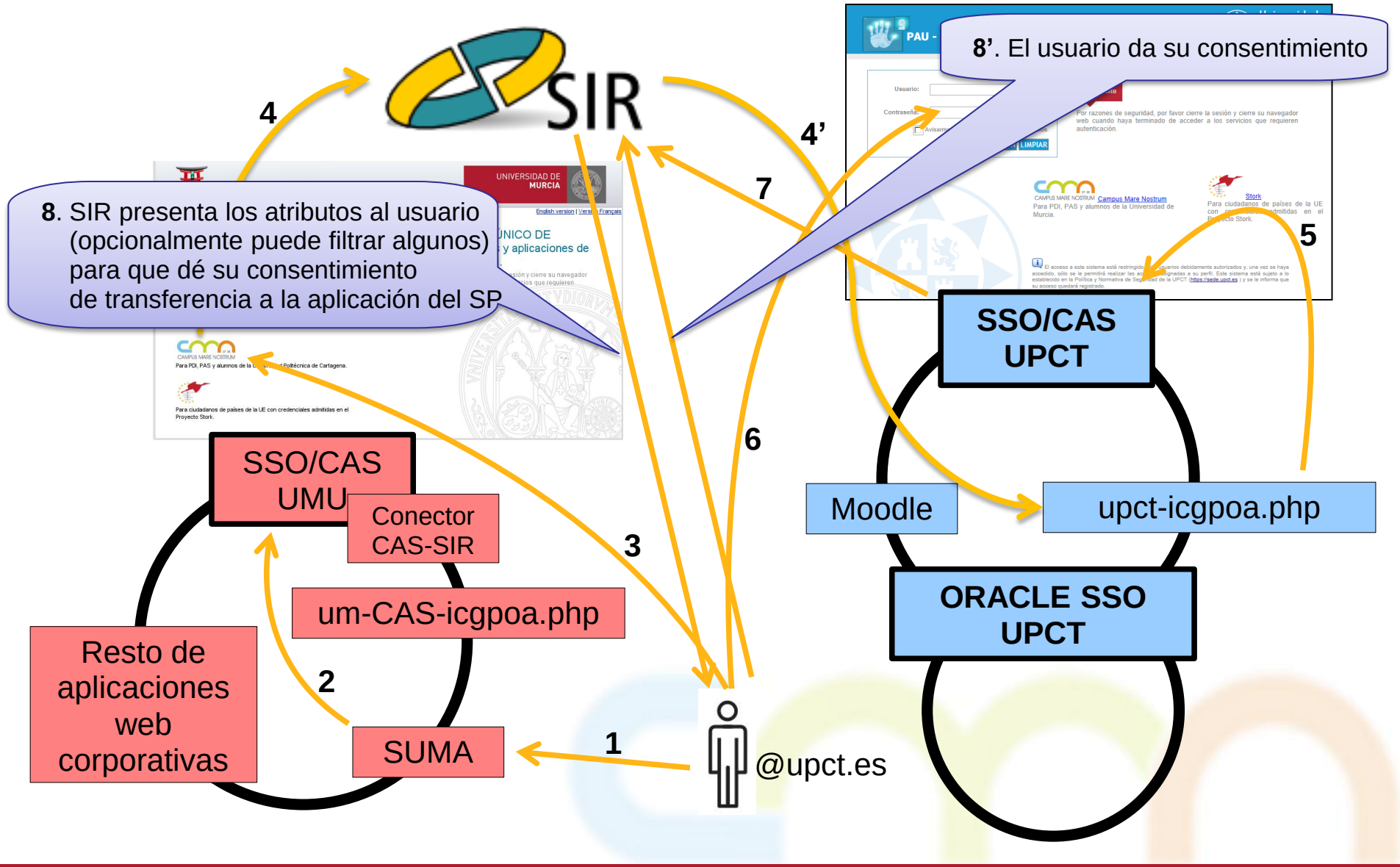
4

4’

5

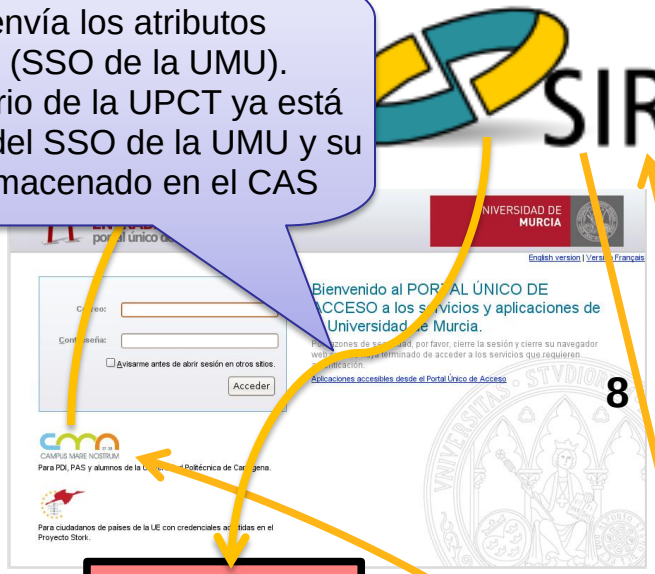
6

9. Ejemplo de uso de la Federación CMN



9. Ejemplo de uso de la Federación CMN

9. SIR envía los atributos al SP (SSO de la UMU). El usuario de la UPCT ya está dentro del SSO de la UMU y su perfil almacenado en el CAS



SIR

SSO/CAS UMU

Conector CAS-SIR

um-CAS-icgpoa.php

Resto de aplicaciones web corporativas

SUMA

@upct.es

SSO/CAS UPCT

Moodle

upct-icgpoa.php

ORACLE SSO UPCT

1

2

3

4’

5

6

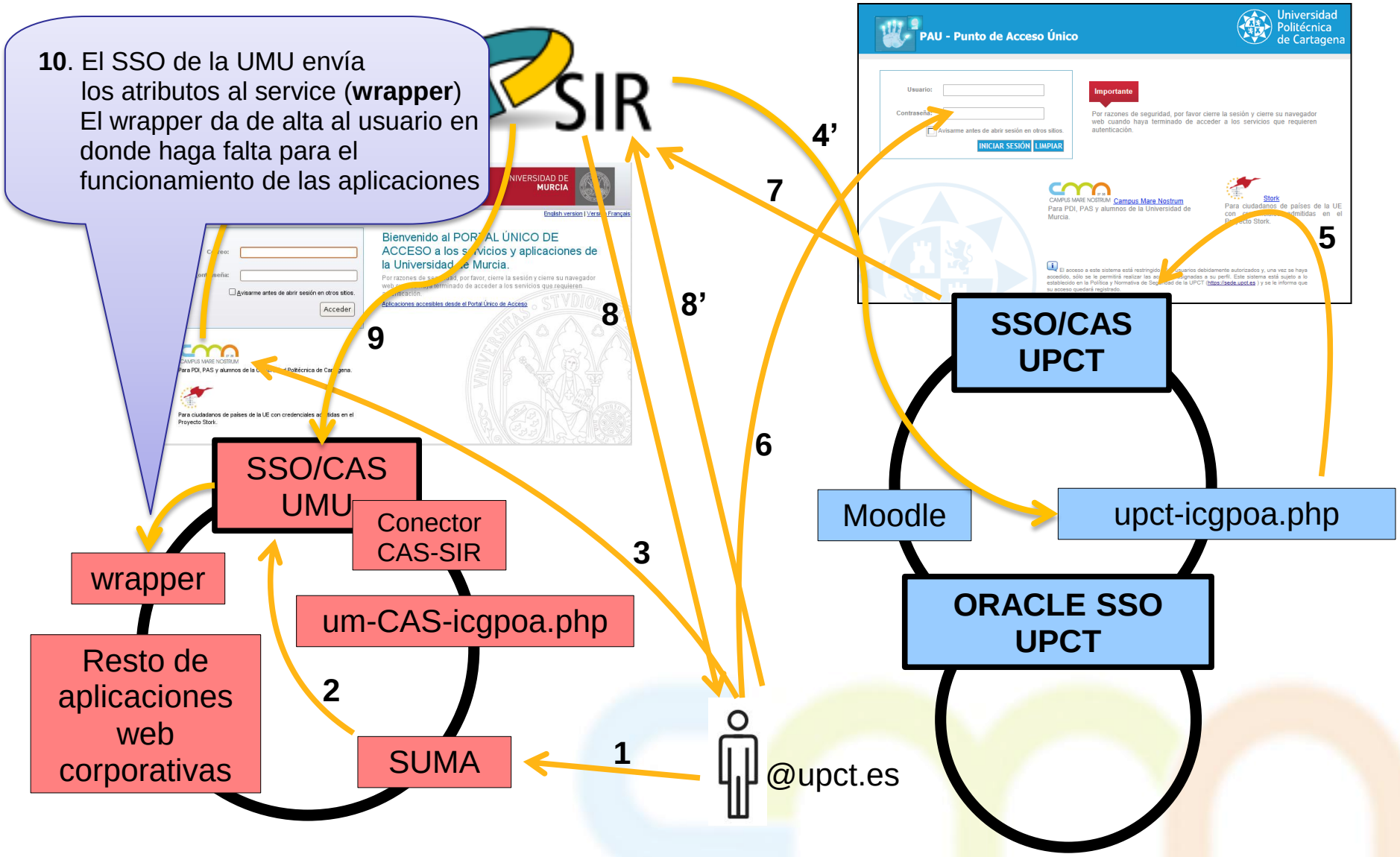
7

8

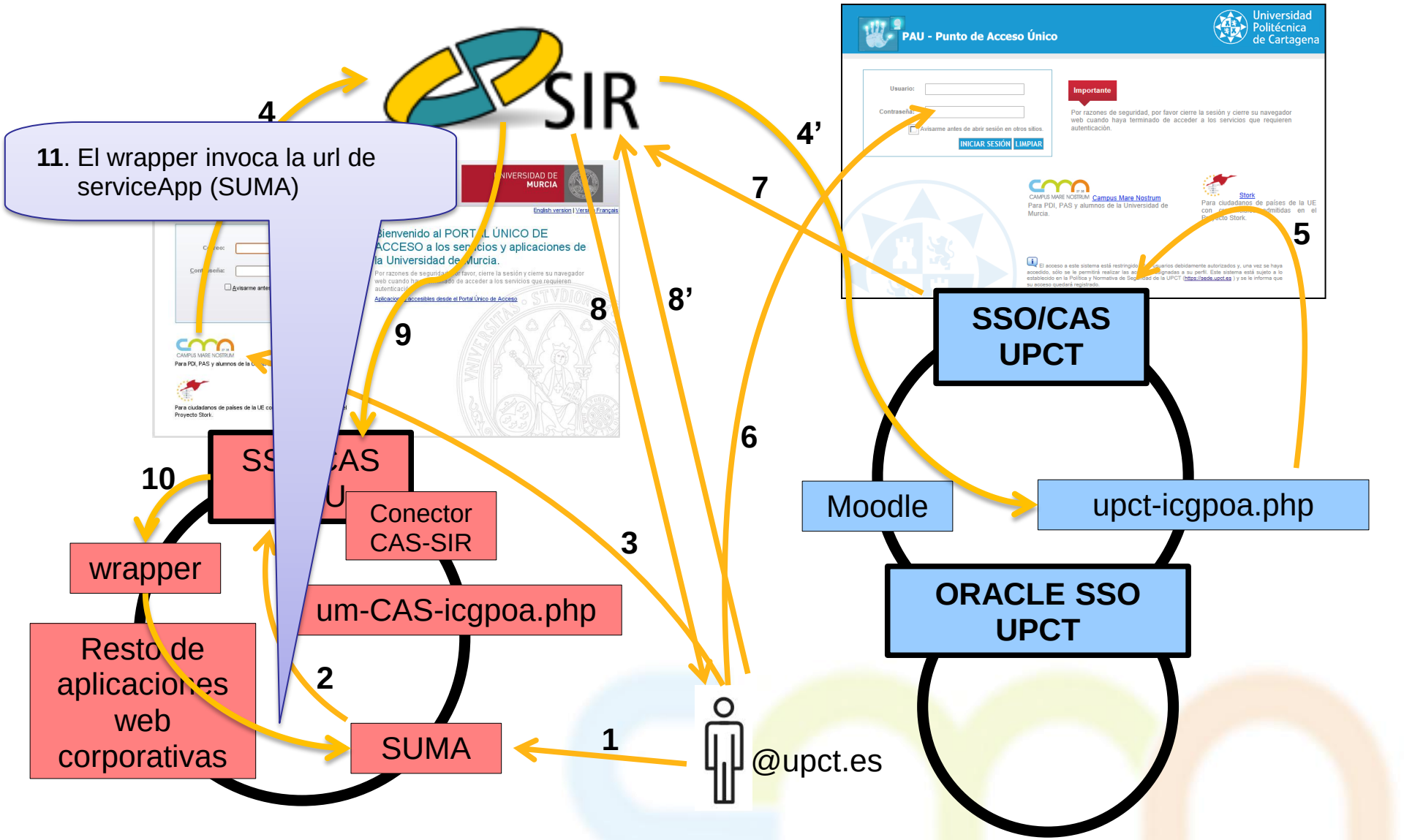
8’

9. Ejemplo de uso de la Federación CMN

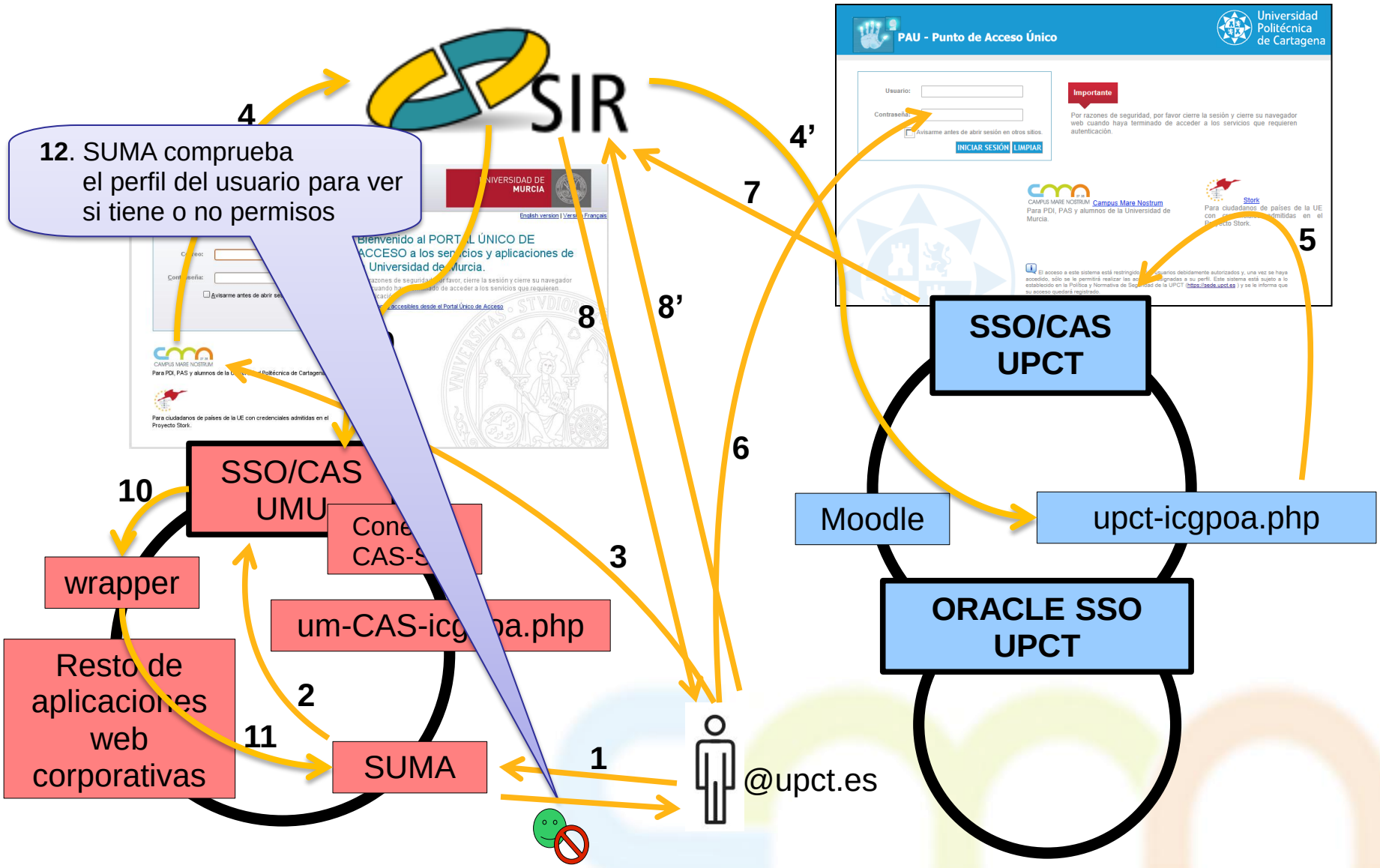
10. El SSO de la UMU envía los atributos al service (**wrapper**) El wrapper da de alta al usuario en donde haga falta para el funcionamiento de las aplicaciones



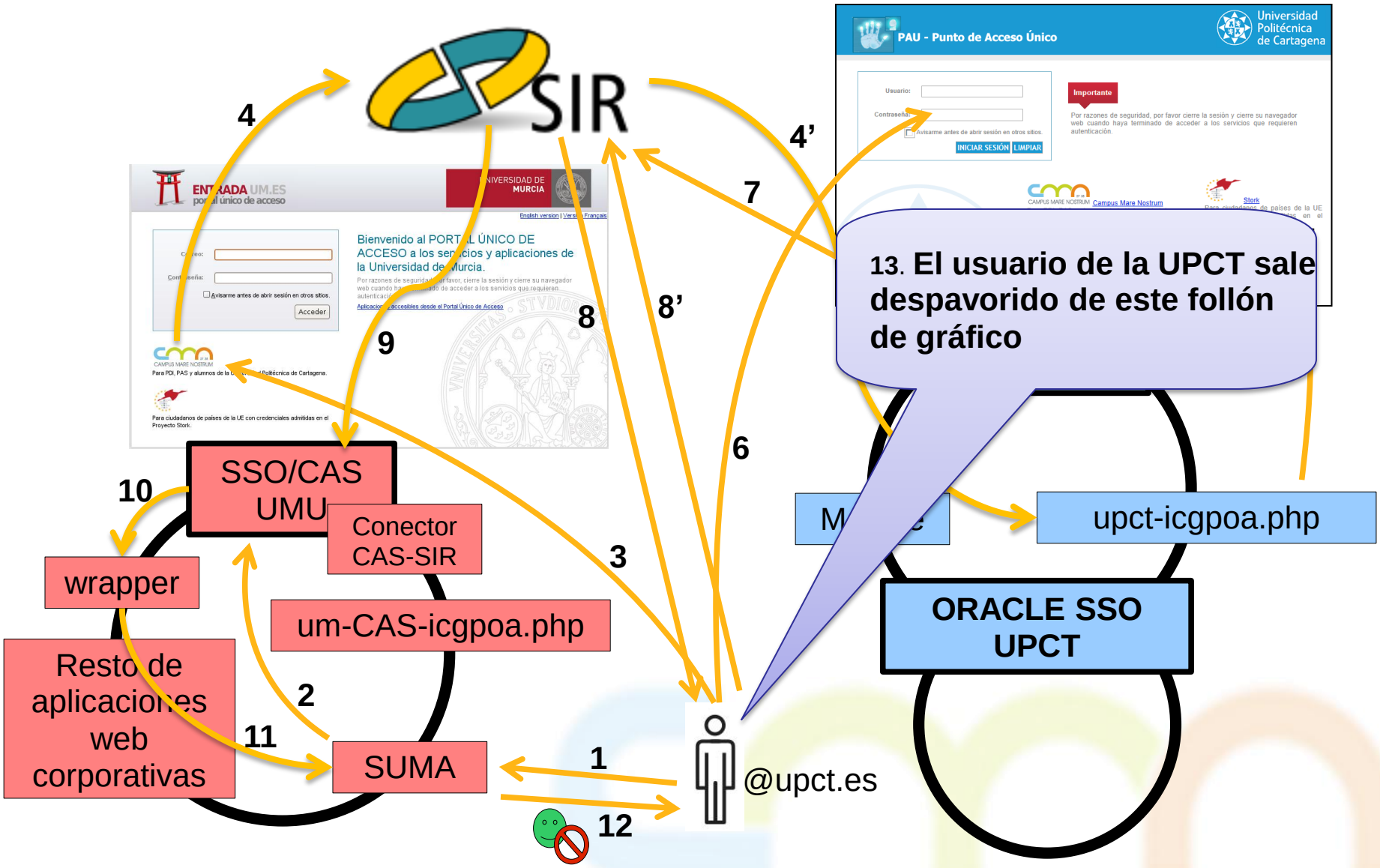
9. Ejemplo de uso de la Federación CMN



9. Ejemplo de uso de la Federación CMN



9. Ejemplo de uso de la Federación CMN



10.- Futuro

10. Futuro

- Inmediato: puesta en marcha de la federación (con aplicaciones reales).
- Revisión y normalización de atributos SIR.* a intercambiar entre la UPCT y la UMU.
- Uso de certificados digitales.
- Conexión a otros sistemas de autenticación y autorización federados (OpenID, Live@EDU, ...)
- Incorporación de más IdPs a la federación

11.- Enlaces de Interés

11. Enlaces de Interés

- Campus Mare Nostrum: http://www.**campusmarenostrum**.com
- Servicio de Identidad de RedIris y PAPI
  - http://www.rediris.es/**sir**/
  - http://www.rediris.es/actividades/**papi**/
- CAS Jasig:
  - http://www.jasig.org/**cas**
  - *https://wiki.jasig.org/display/**CAS**/**CASifying**+**Oracle**+Portal*
- Proyecto europeo STORK: https://www.eid-stork.eu/
- Identificación en la USC. Identificación federada mediante SIR/STORK.
  - http://www.rediris.es/jt/jt2010/ponencias/jt2010-jt-serv_feder_1-2.pdf
  - *https://**forja**.rediris.es/projects/**cas-sir-stork**/*
- SAML (Security Assertion Markup Language): http://saml.xml.org/
- Oracle Application Server: http://download.oracle.com/docs/cd/B15904_01/index.htm
- Memcached: http://www.**memcached**.org
- Librería Inspektr, para auditoría: http://code.google.com/p/**inspektr**/

12.- Conclusiones

11. Conclusiones

- Rápida puesta en marcha de un entorno federado (“encaje de piezas”, desarrollo mínimo)
- Incorporación fácil de nuevas funcionalidades al CAS
- El wrapper nos permite dar de alta los perfiles mínimos imprescindibles para el funcionamiento de las aplicaciones federadas
- SIR se revela como una infraestructura adecuada para la creación de sub-federaciones
- Ahorro de costes y esfuerzo por uso de infraestructura ya existente (SIR)

13.- Agradecimientos

12. Agradecimientos

- Diego López (RedIRIS)
- Jaime Pérez (RedIRIS)
- Diego Conde (USC)

¡¡ Muchas gracias por todo !!

¿PREGUNTAS?