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

RedIRIS

Cuenca

5 y 6 de octubre 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/

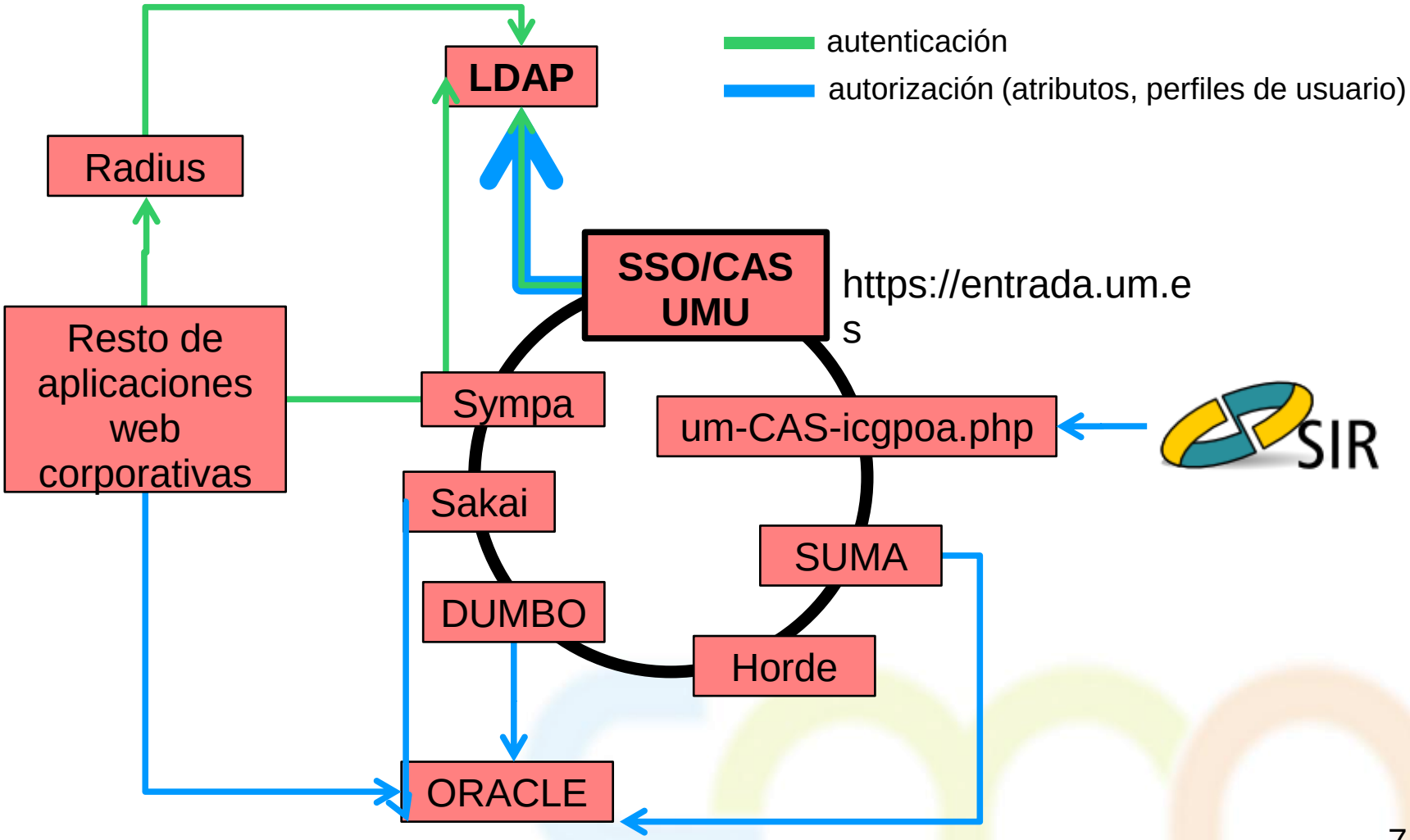
"**Campus Mare Nostrum 37/38** es el Campus de Excelencia Internacional de la Universidad de Murcia y la Universidad Politécnica de Cartagena que, junto a centros de investigación, administraciones públicas, organizaciones internacionales, parques tecnológicos y empresas, persigue transformar la Región 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 (algunas vía RADIUS).
  - Atributos de usuario (perfiles) en Open LDAP y BBDD ORACLE.

Universidad de Murcia (enero 2011)

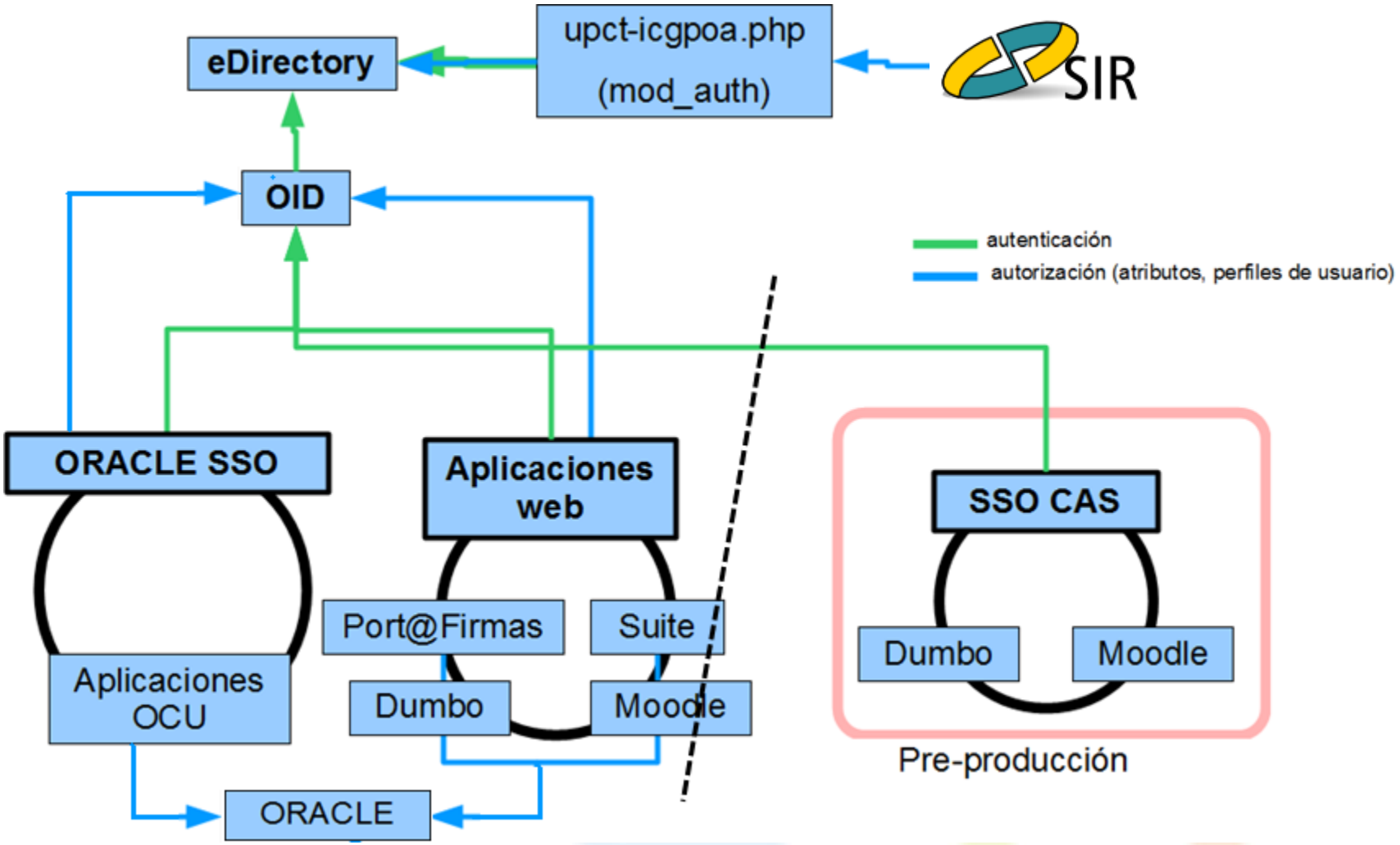


Universidad Politécnica de Cartagena (enero 2011)

- IdP de SIR desde enero de 2010. No es **SP** en **SIR.**
- Se usan dos directorios LDAP sincronizados y conectados:
  - El eDirectory de Novell almacena las credenciales de los usuarios. Usado para servicios de red (carpetas en 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.**

2. Situación de partida

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 generación 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 comprobar 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 "retocable".
- 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).**

Características de CAS-Jasig

- Puede enlazar con distintas fuentes de autenticación (Active Directory, JAAS, JDBC, LDAP, RADIUS, Trusted, Certificados X.509).
- Proporciona librerías para Apache, .Net, PHP y Java, que simplifican la adaptación de las aplicaciones al CAS.
- Genera aserciones con protocolo SAML 1.1 y SAML 2.0.
  - SAML 1.1: Está soportado por Java CAS Client 3.1.x, phpCAS 1.1.0, mod_auth_cas 1.09 y .Net Cas Client.
  - SAML 2.0: Probado únicamente con Google Apps.
- Las aplicaciones **no tienen acceso a las credenciales.**
- La información de identidad puede complementarse con atributos.

Extensiones de Seguridad

- **LDAP Password Policy Enforcement**
  - Extensión para prevenir el cumplimiento de políticas de contraseñas establecidas en LDAP (propuesta para la v3.5.).
    - Mensajes de aviso del tipo: la contraseña va a expirar en <X< días; la contraseña ha expirado y debe resetearla; cuenta bloqueada; y cuenta desactivada.

- **Throttling Login Attempts**
  - Extensión para prevención de ataques por diccionario.
  - Funcionamiento: Algoritmo de estrangulamiento por intentos de accesos fallidos.

1º fallo de acceso	Sin retraso
2º fallo de acceso	2 sec de retraso
3º fallo de acceso	4 sec de retraso
4º fallo de acceso	8 sec de retraso
...	...

Gestión de Tickets CAS-Jasig

- En memoria (por defecto):
  - Sencilla y suficiente para la mayoría.
  - No permite ajustar al CAS para un rendimiento óptimo.

- Con **Memcached**: sistema distribuido de propósito general de cachés basado en memoria.
  - Almacena los tickets, descargando al CAS de esta tarea.
  - Es independiente del funcionamiento del CAS.
  - Permite crear una instancia CAS multi-nodo.
  - Permite reiniciar nodos del CAS sin perdida de sesión, lo que facilita el mantenimiento de los nodos del CAS.
  - No failover. Para eso usar Repcached.

- Otros métodos de registro de tickets: JPA,...

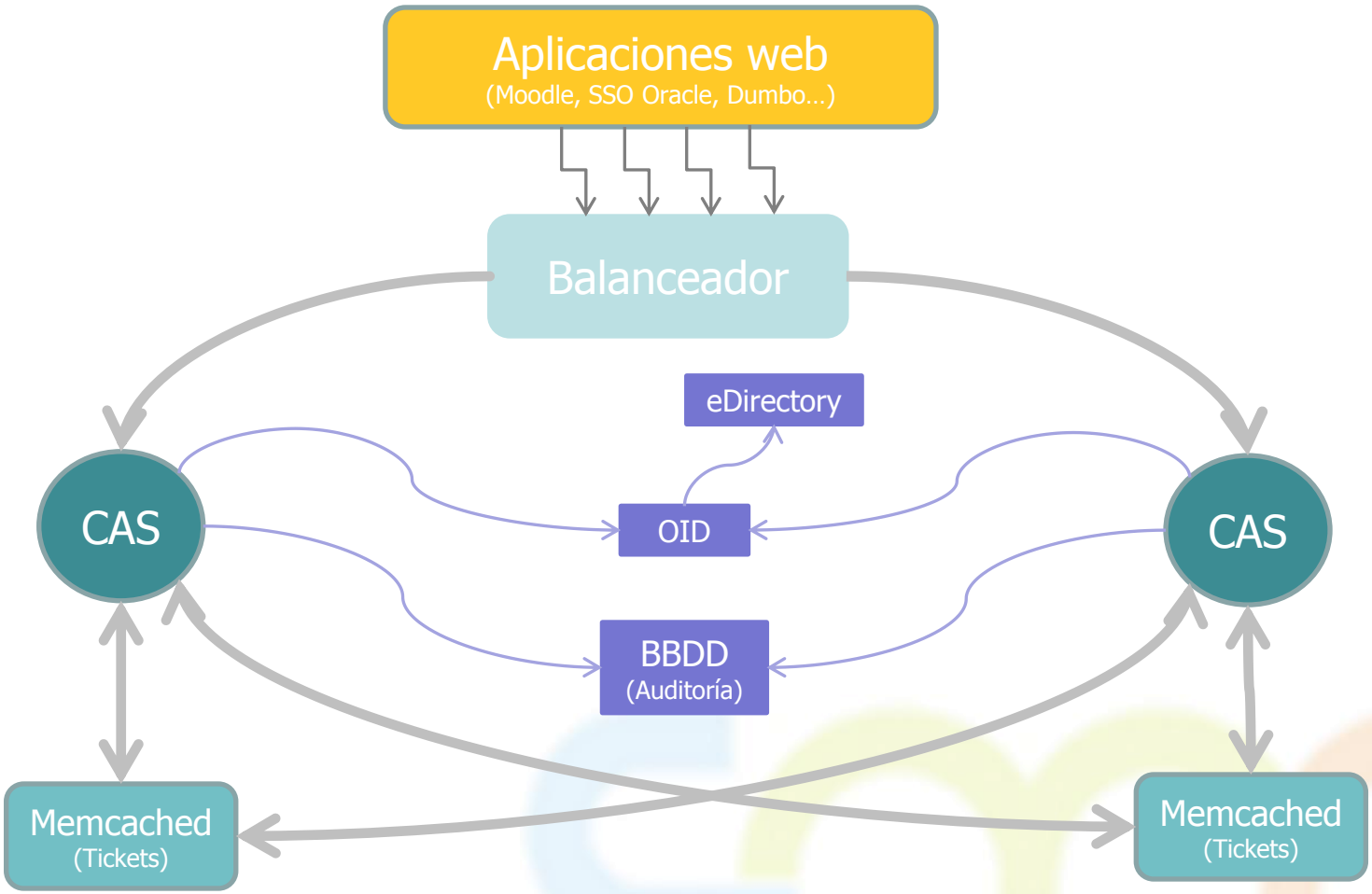
Expiración de Tickets y Auditoría

- **Política de Expiración de Tickets:**
  - Último uso del ticket.
  - Tiempo que lleva el ticket creado .
  - Número máximo de veces que se puede utilizar un ticket.

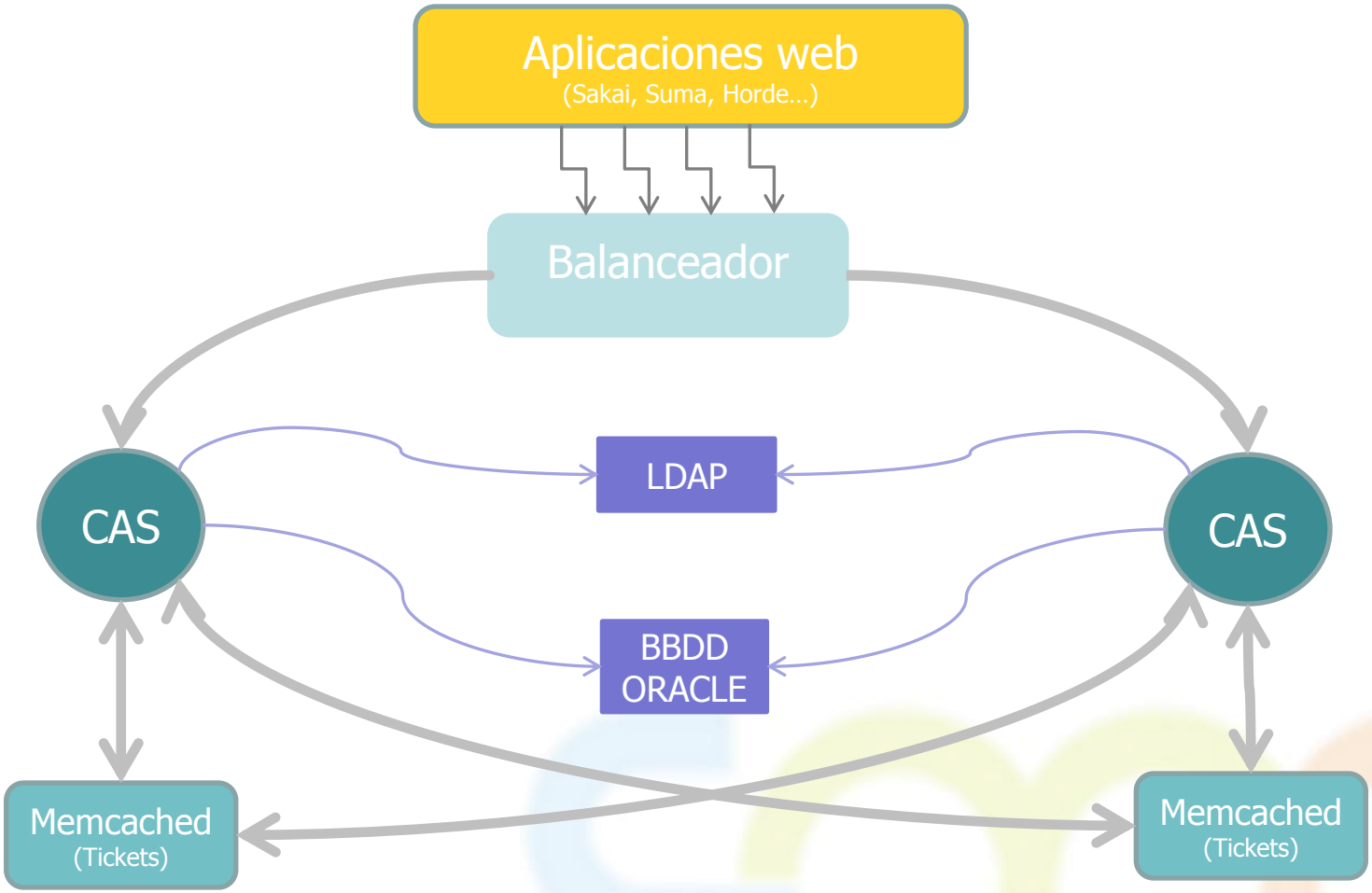
- **Auditoría con Inspektr:**
  - Auditoría no intrusiva.
  - Registro de las rutas de ejecución.
  - Registro en ficheros o en base de datos (MySQL, Oracle, …).

AUD_USER	AUD_CLIENT_IP	AUD_SERVER_IP	AUD_RESOURCE	AUD_ACTION	APP	AUD_DATE
[username: 77521462]	212.128.20.201	212.128.20.238	supplied credentials: [username: 77521462]	AUTHENTICATION_SUCCESS	CAS	20/09/2011 12:53
[username: 77521462]	212.128.20.201	212.128.20.238	TGT-10-bgE5ZO0dMQXl0JmKWdmBeduLdM2TepXjuNVHRZIgaKYNt	TICKET_GRANTING_TICKET_CREATED	CAS	20/09/2011 12:54
77521462P	212.128.20.201	212.128.20.238	ST-11-Dfe1d4AkNeFqFCdp9ytq-casW09 for https://dumbo.upct.es/	SERVICE_TICKET_CREATED	CAS	20/09/2011 12:55
audit:unknown	212.128.20.201	212.128.20.203	ST-11-Dfe1d4AkNeFqFCdp9ytq-casW09	SERVICE_TICKET_VALIDATED	CAS	20/09/2011 12:55
audit:unknown	212.128.20.201	212.128.20.203	TGT-51-1fewDJC1kwLKDijiB3pPf2Zw1iuRcT6qzKbgEvxFcY7tZhel7G-	TICKET_GRANTING_TICKET_DESTROYE	CAS	20/09/2011 12:55
[username: 27457677-N]	212.128.20.201	212.128.20.203	supplied credentials: [username: 27457677-N]	AUTHENTICATION_FAILED	CAS	20/09/2011 16:50
[username: 27457677-N]	212.128.20.201	212.128.20.203	error.authentication.credentials.bad	TICKET_GRANTING_TICKET_NOT_CREA	CAS	20/09/2011 16:50

Arquitectura del SSO/CAS en la UPCT



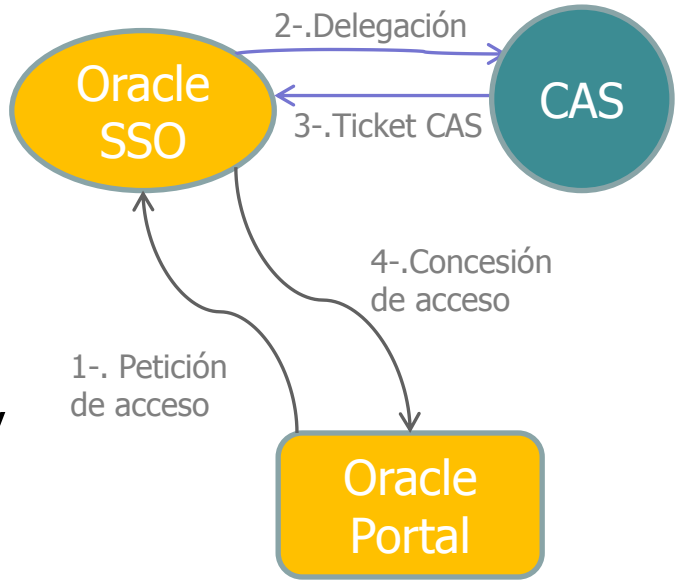
Arquitectura del SSO/CAS en la UMU



6.- “Caseizando” el SSO de Oracle

En que consiste Caseizar el SSO de Oracle:

1. En aplicar un **filtro CAS** a la aplicación Oracle SSO (modificación del web.xml del sso de oracle).
2. Sustituir el plugin Oracle SSO por **el plugin CASAutenticator** (copiar librerías y modificar el fichero policy.properties).
3. Crear un **OC4J público** para la página de desconexión.



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.

- Alta de usuarios en OID mediante un WS invocado desde la aplicación federada.

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

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.

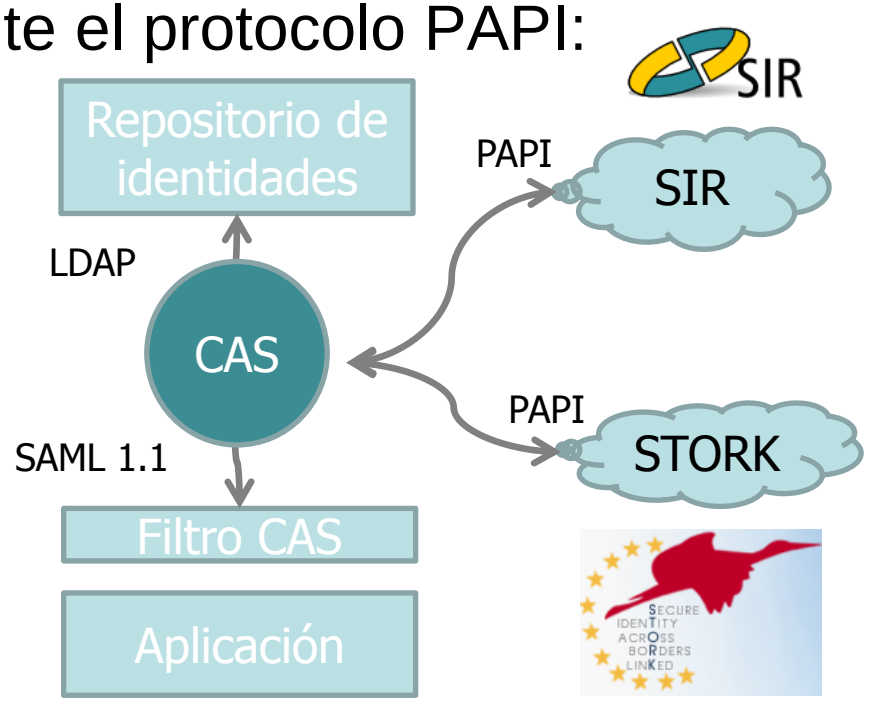
La extensión también tiene ofrece soporte para **STORK**, donde se usan los sistema de identificación electrónica nacionales de cada estado miembro de la UE.

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

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.

Modificaciones y mejoras realizadas en el conector CAS-SIR/STORK de la USC:

- Evitar elección de IdP por parte del usuario en el WAYF (sólo dos organizaciones federadas), gracias al uso del atributo **PAPIHLI** en la URL del servicio CAS.

- Modificaciones del código del conector CAS-SIR/STORK, para poder elegir el IdP bien desde la aplicación o bien desde el CAS.

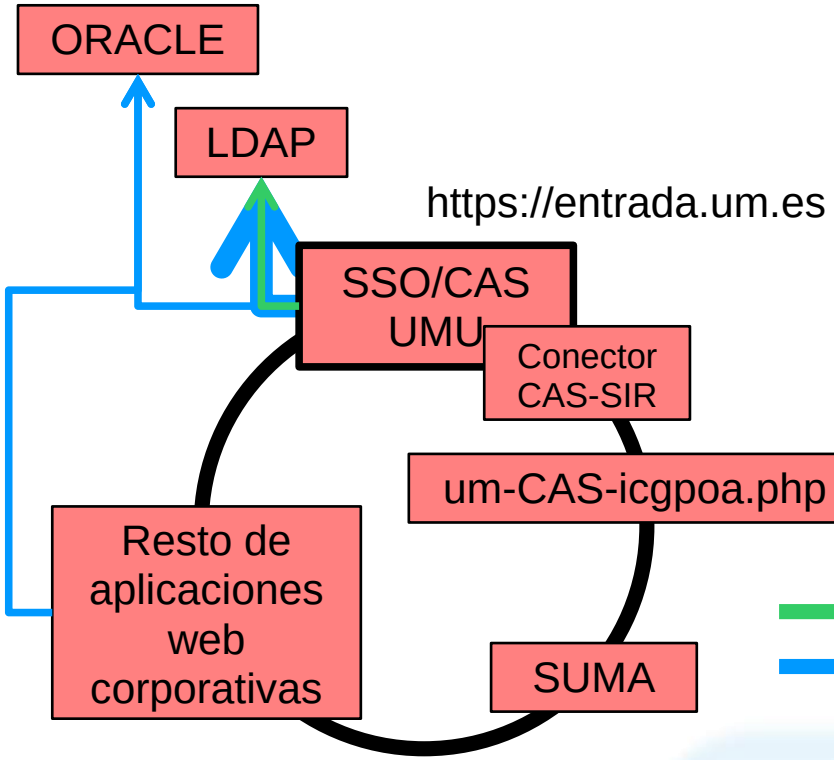
8.- Estado Actual de la Federación CMN

Universidad de Murcia (octubre 2011)

- Todas las aplicaciones en el SSO/CAS
- CAS sigue autenticando contra LDAP
- Aplicación de campus virtual (SUMA) 1ª candidata a federar en CMN
- Conector CAS-SIR probado[1]
- Posibilidad de generar perfiles centralizados en CAS a partir de consultas al LDAP y a ORACLE[1]
- Formulario de entrada modificado para contemplar la federación CMN (y STORK)[1]

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

Universidad de Murcia (octubre 2011)



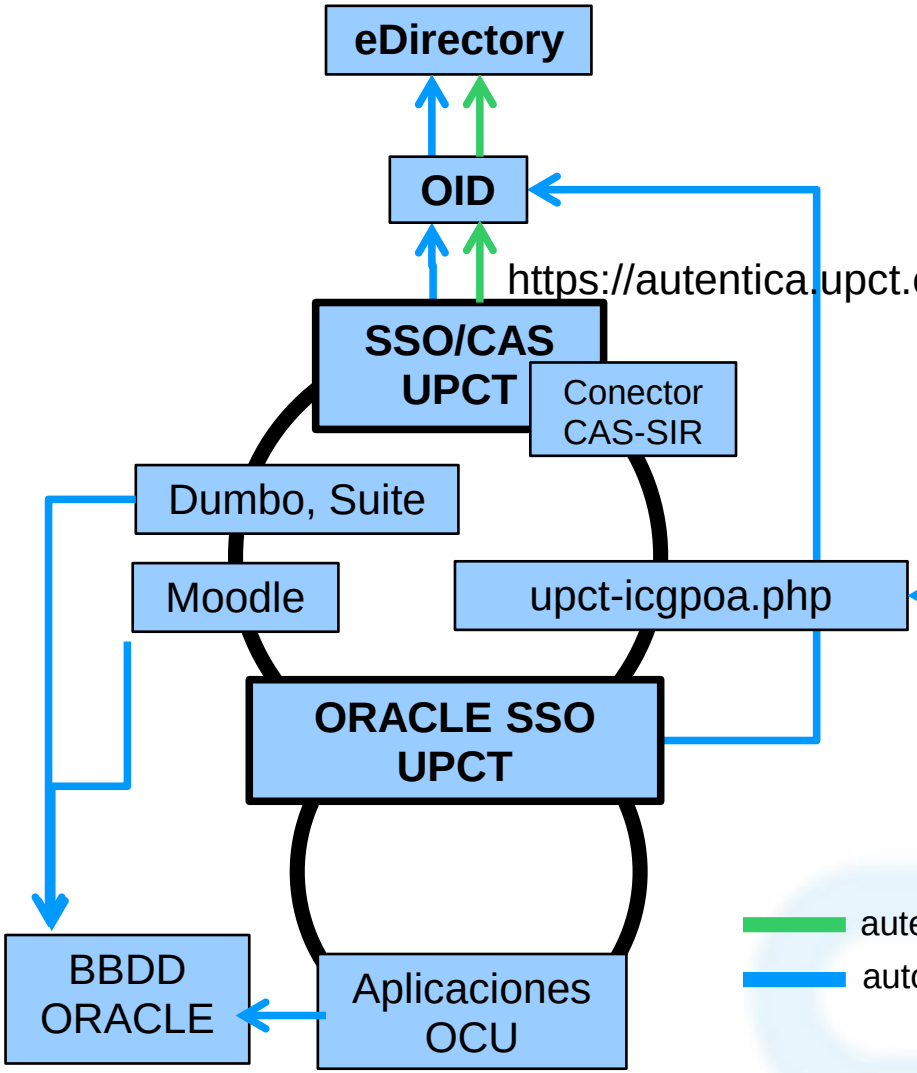
Universidad Politécnica de Cartagena (octubre 2011)

- Todas las aplicaciones ORACLE en el SSO/CAS vía caseización de Oracle SSO. [1]
- Resto de aplicaciones en el SSO/CAS.
- CAS autentica contra OID.
- Moodle y Portal de Servicios, primeros candidatos a federar en CMN.
- Conector CAS-SIR probado.[1]
- Posibilidad de generar perfiles centralizados en CAS a partir de consultas al OID.[1]
- Formulario de entrada modificado para contemplar la federación CMN (y STORK).[1]

1. En entorno de pre-producción

8. Estado actual de la Federación CMN

Universidad Politécnica de Cartagena

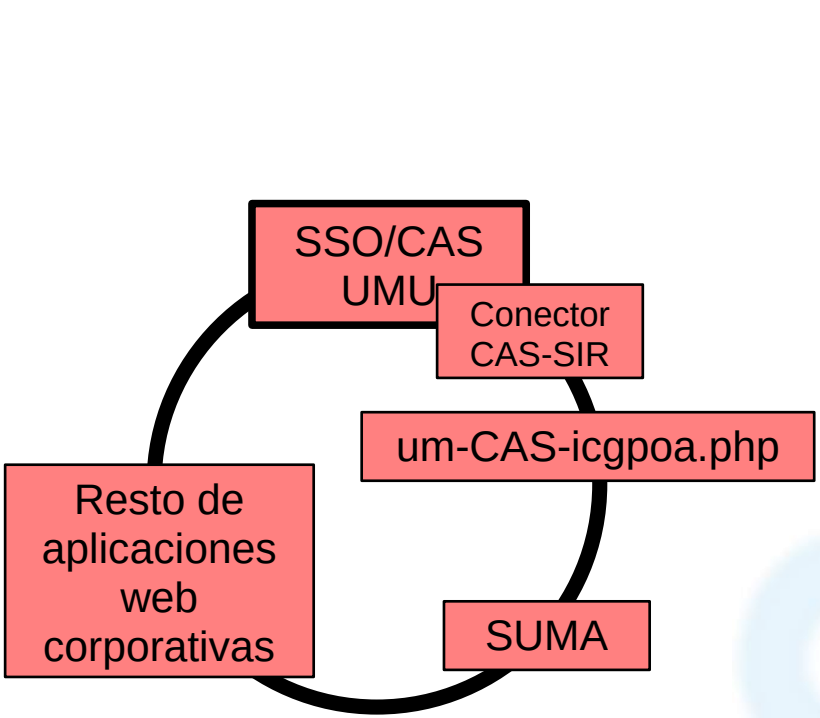


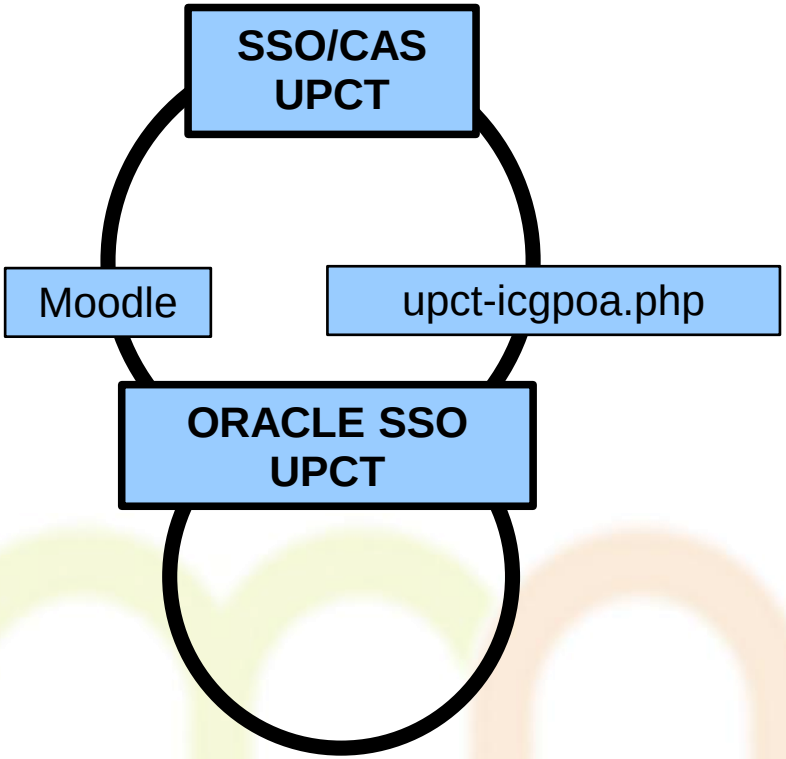
autenticación

autorización (atributos, perfiles de usuario)

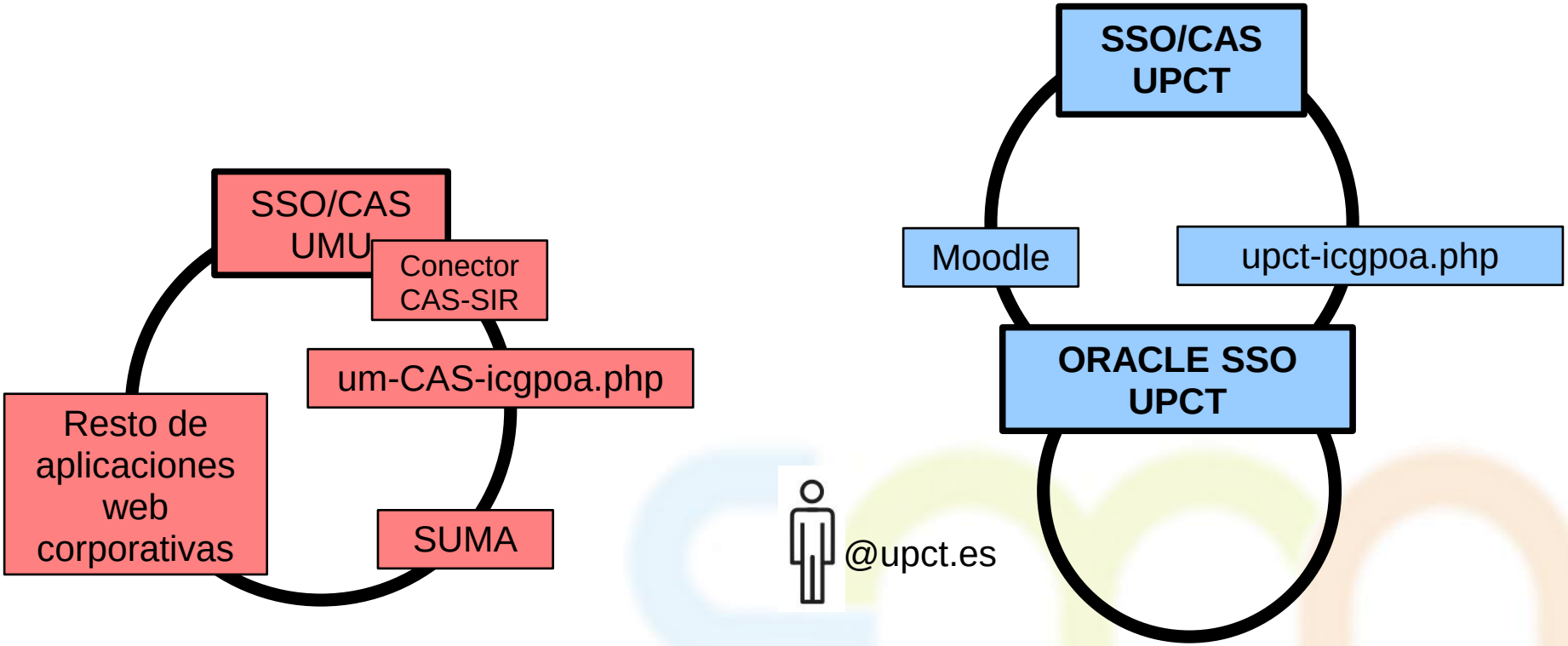
9.- Ejemplo de uso de la Federación CMN

9. Ejemplo de uso de la Federación CMN

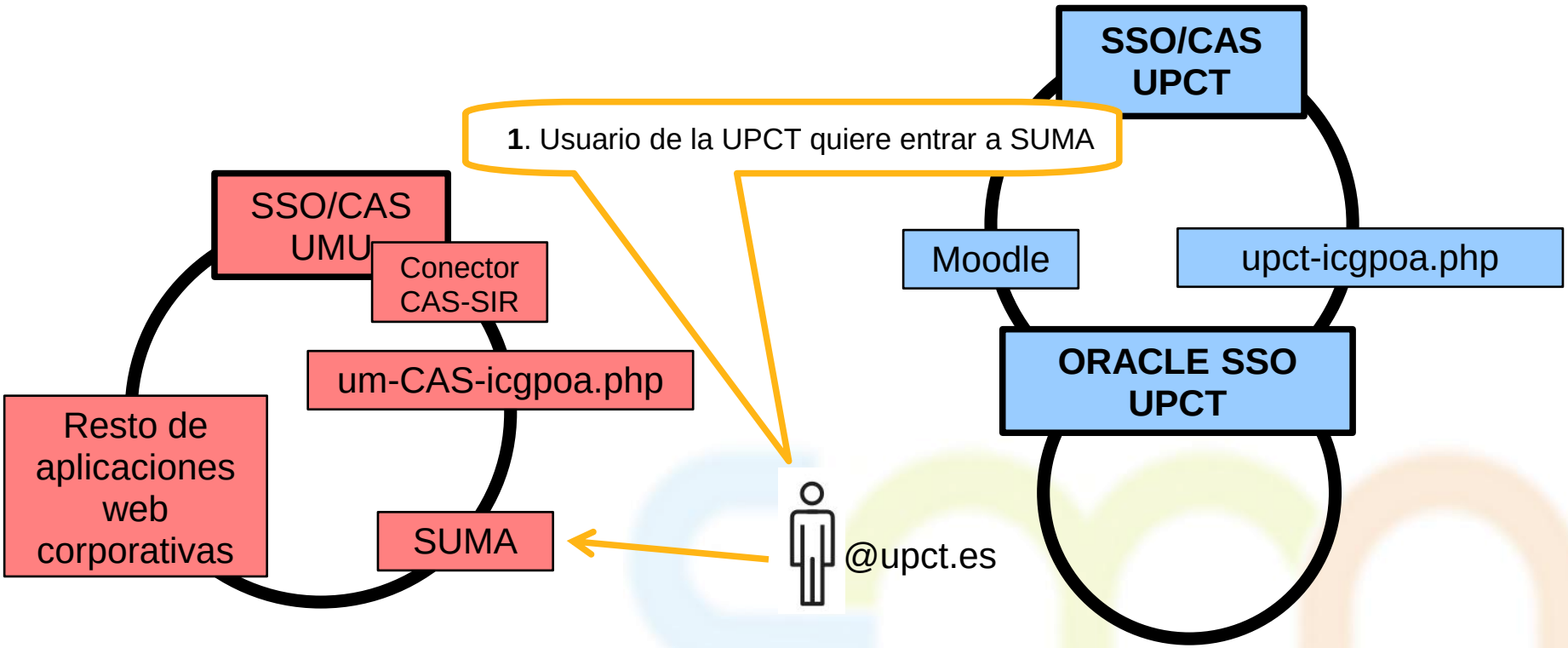




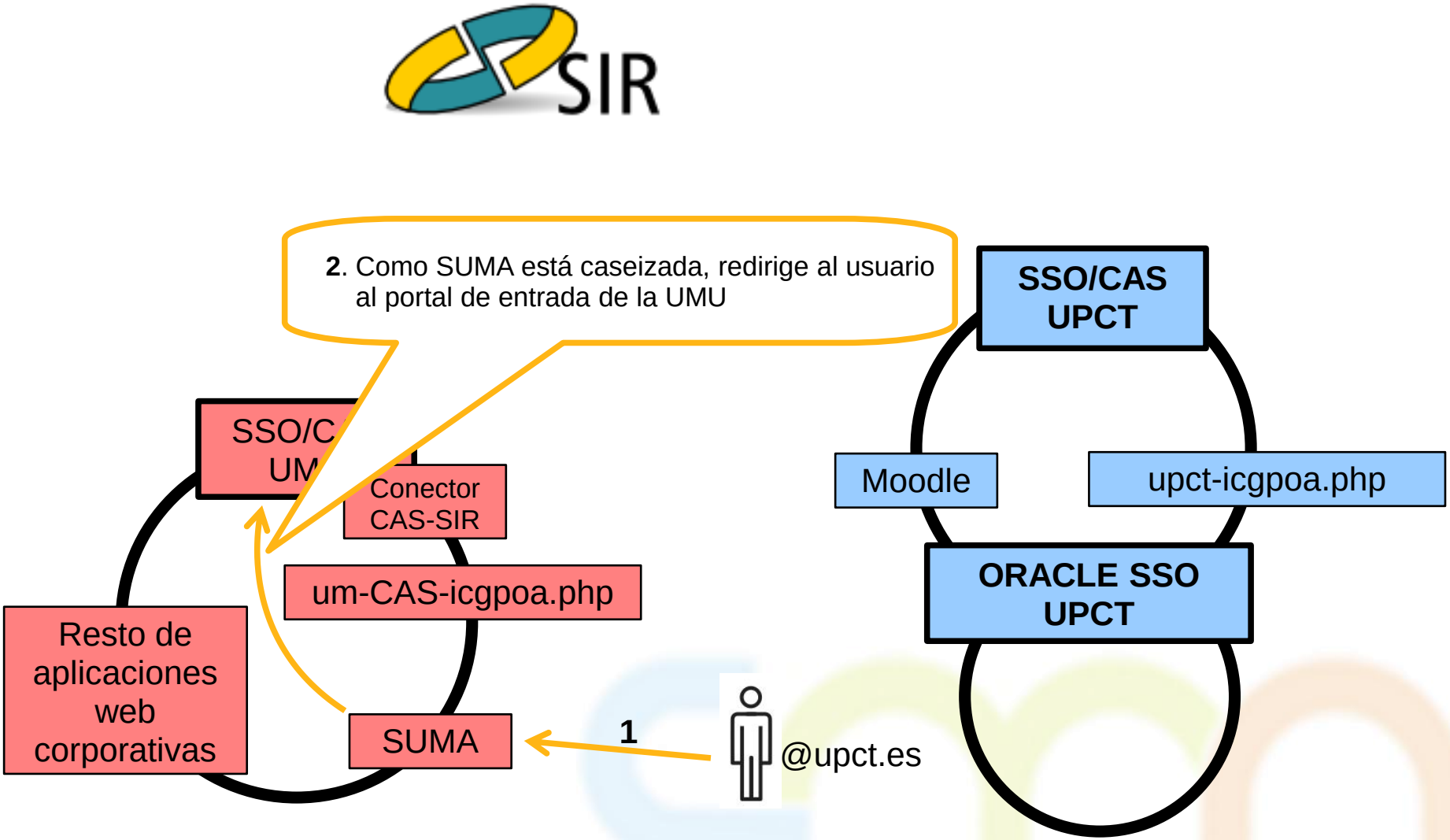
9. Ejemplo de uso de la Federación CMN



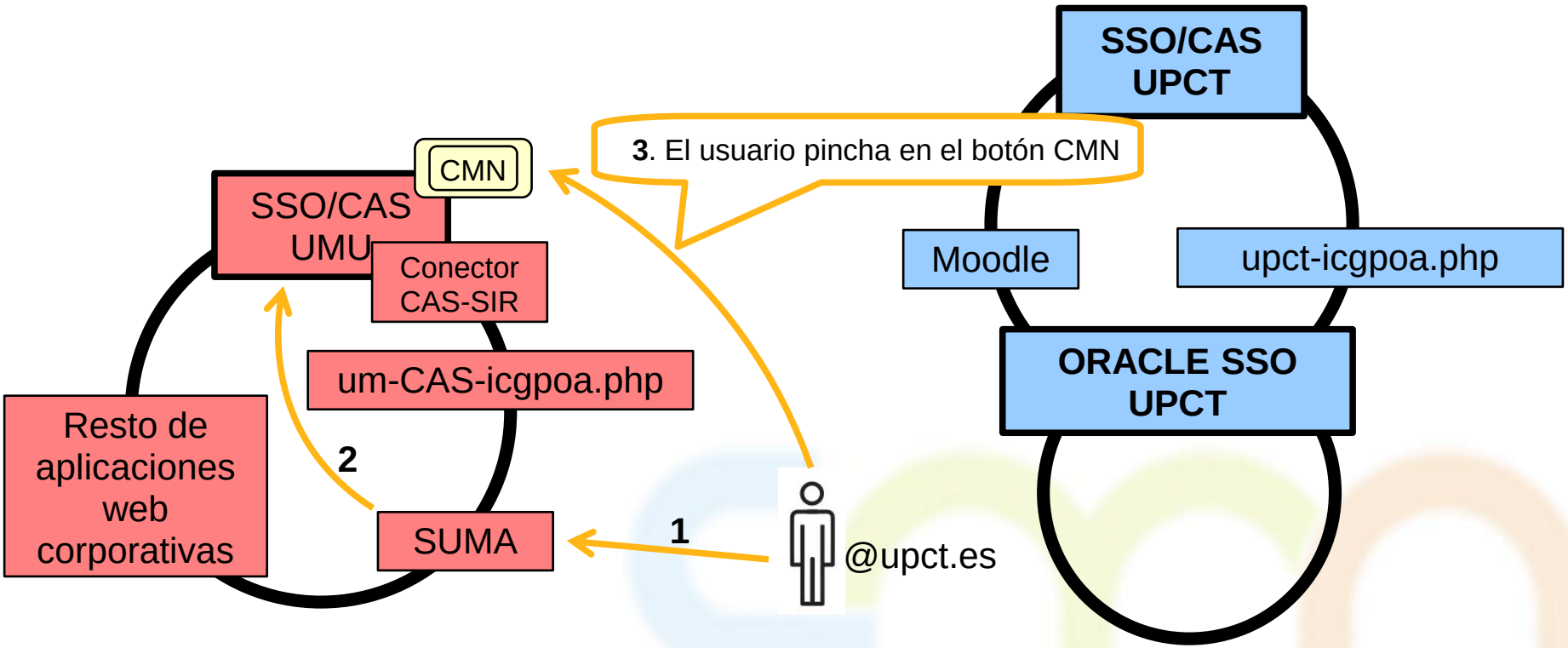
9. Ejemplo de uso de la Federación CMN



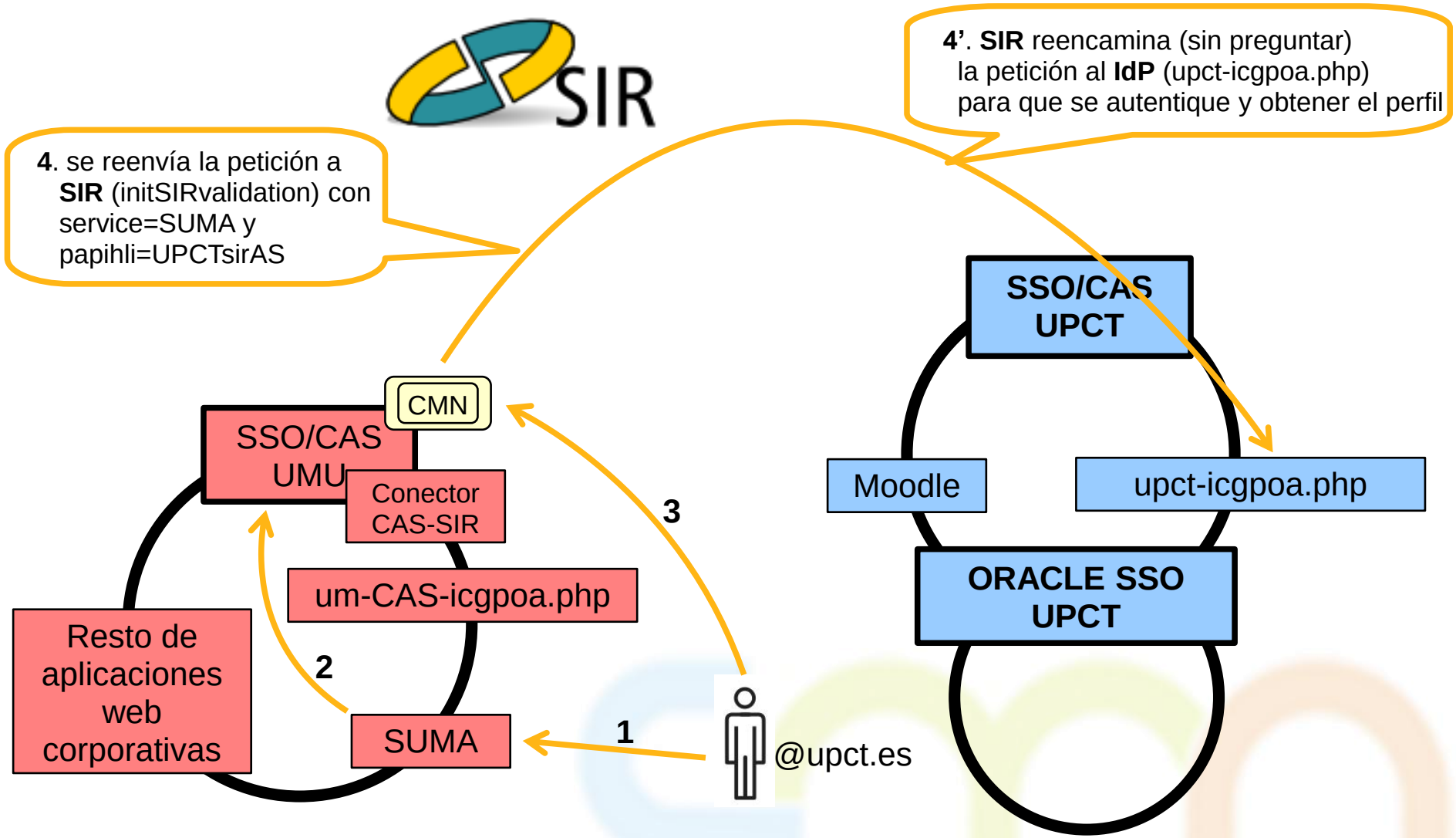
9. Ejemplo de uso de la Federación CMN



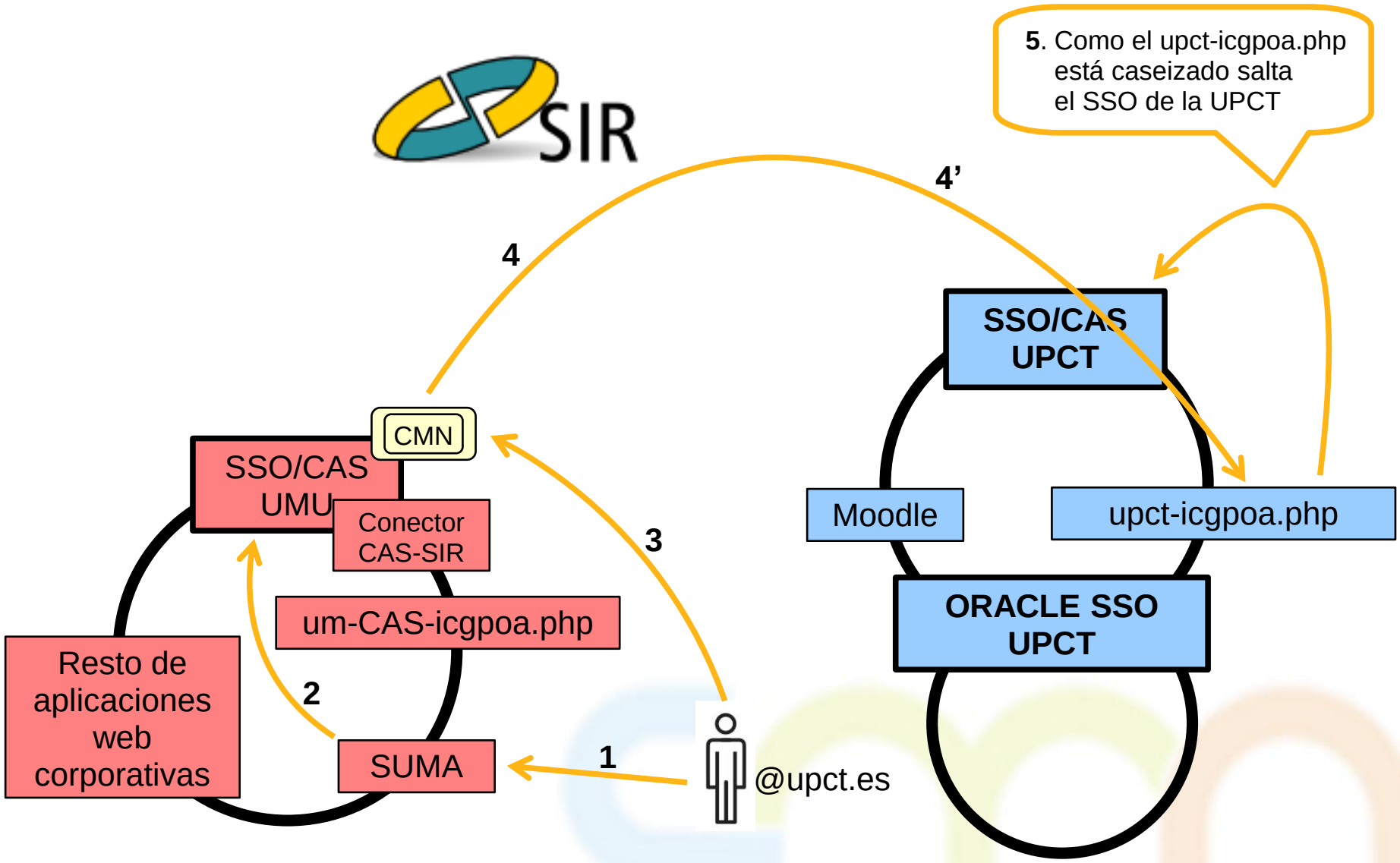
9. Ejemplo de uso de la Federación CMN



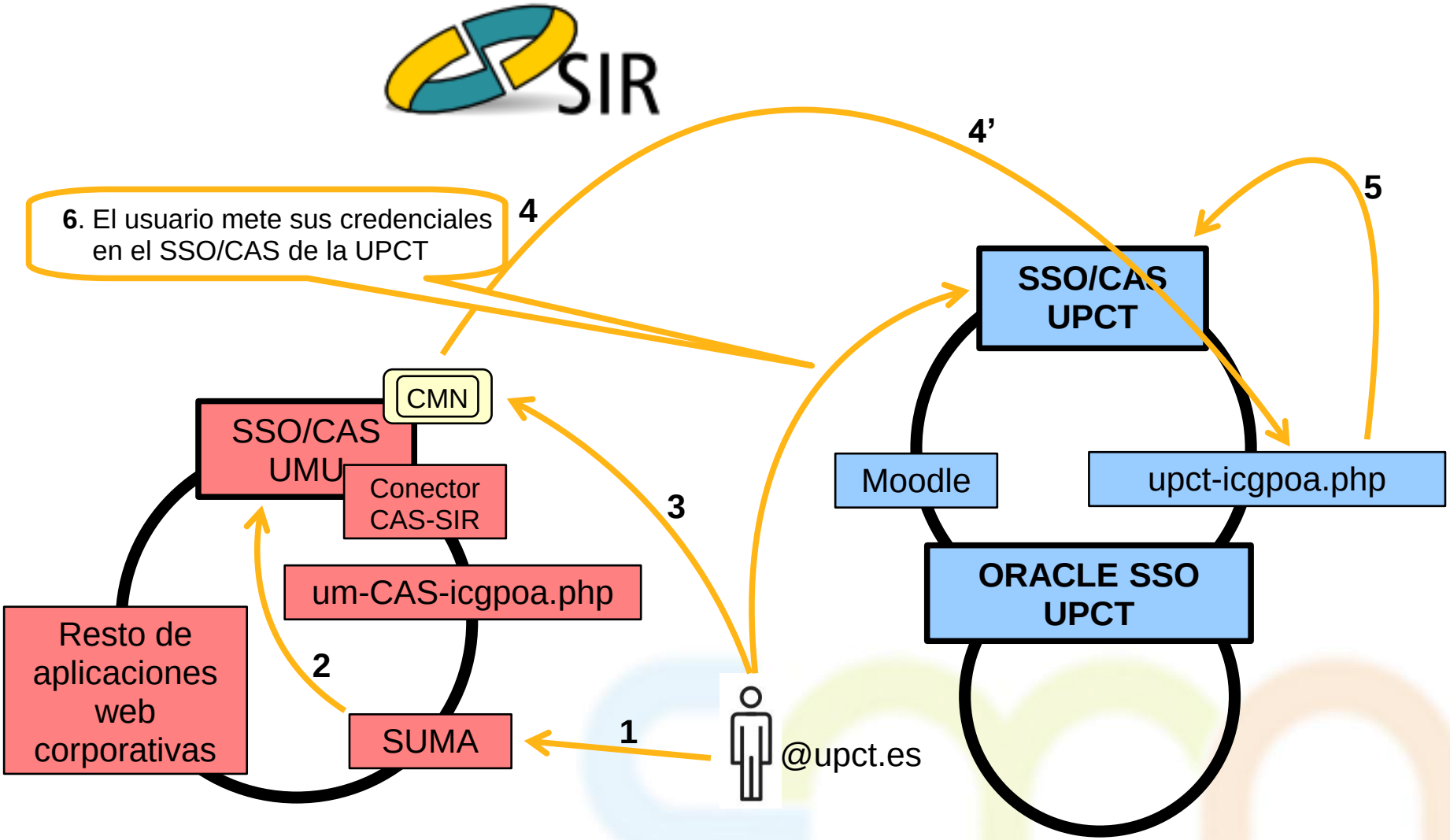
9. Ejemplo de uso de la Federación CMN



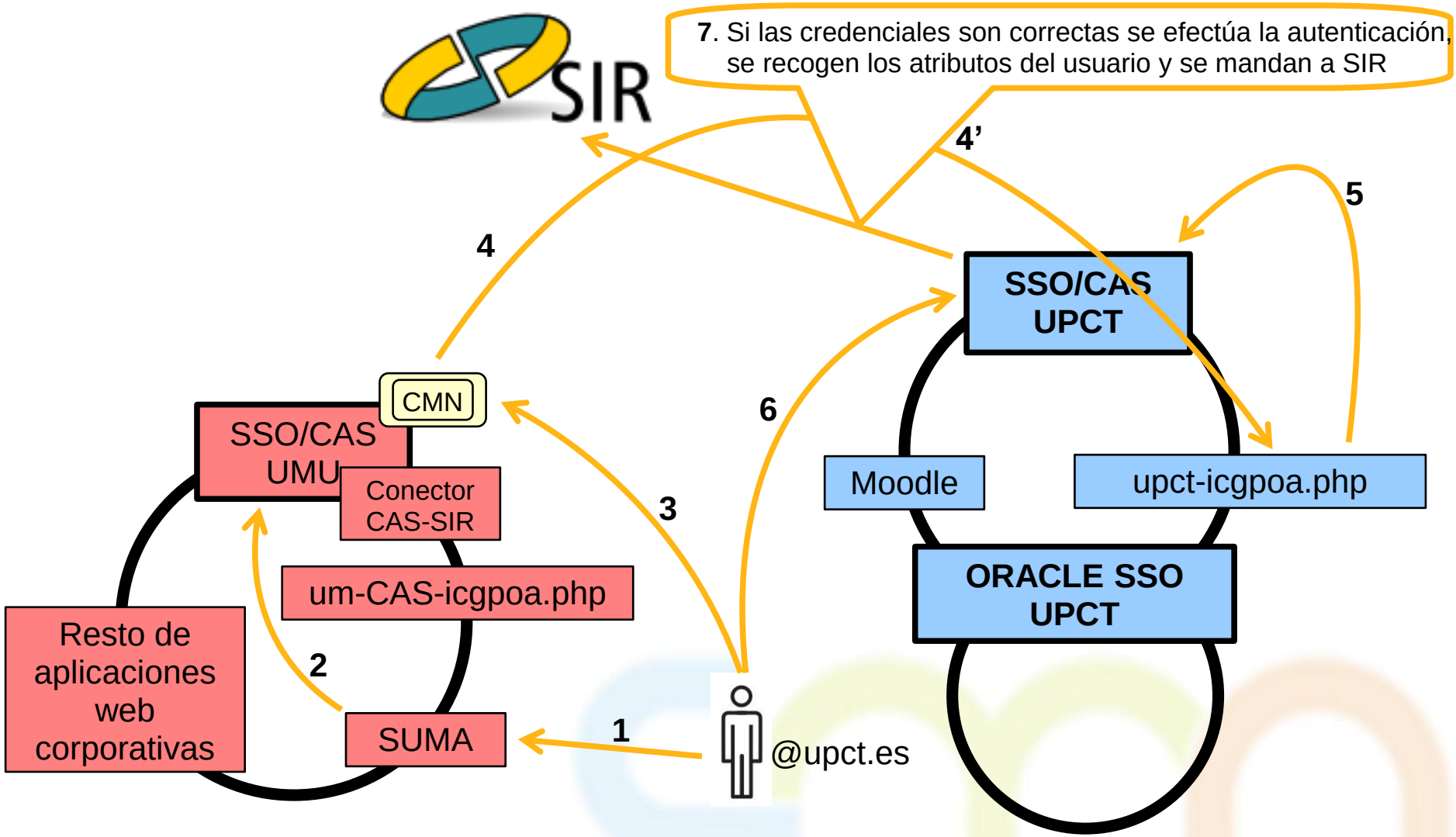
9. Ejemplo de uso de la Federación CMN



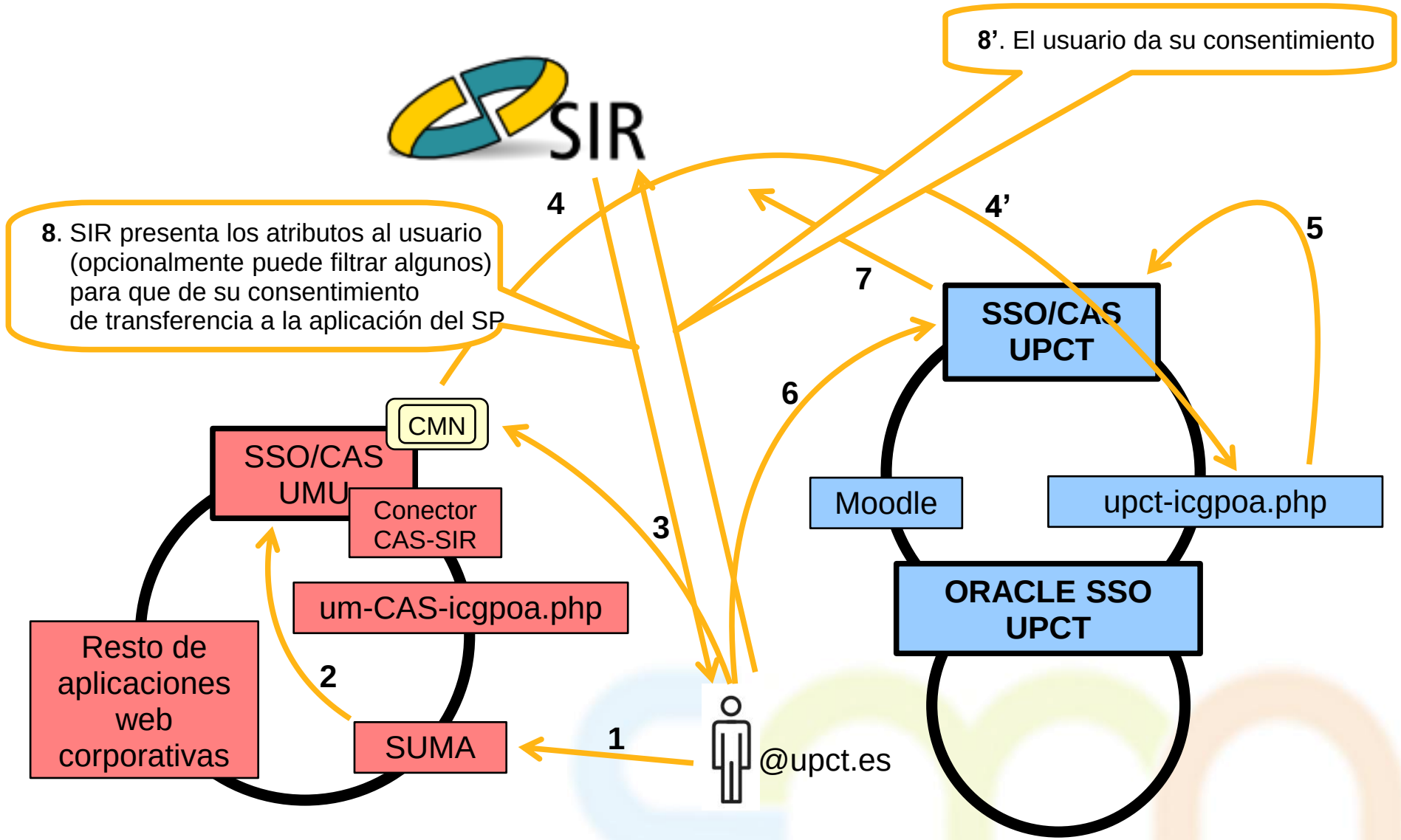
9. Ejemplo de uso de la Federación CMN



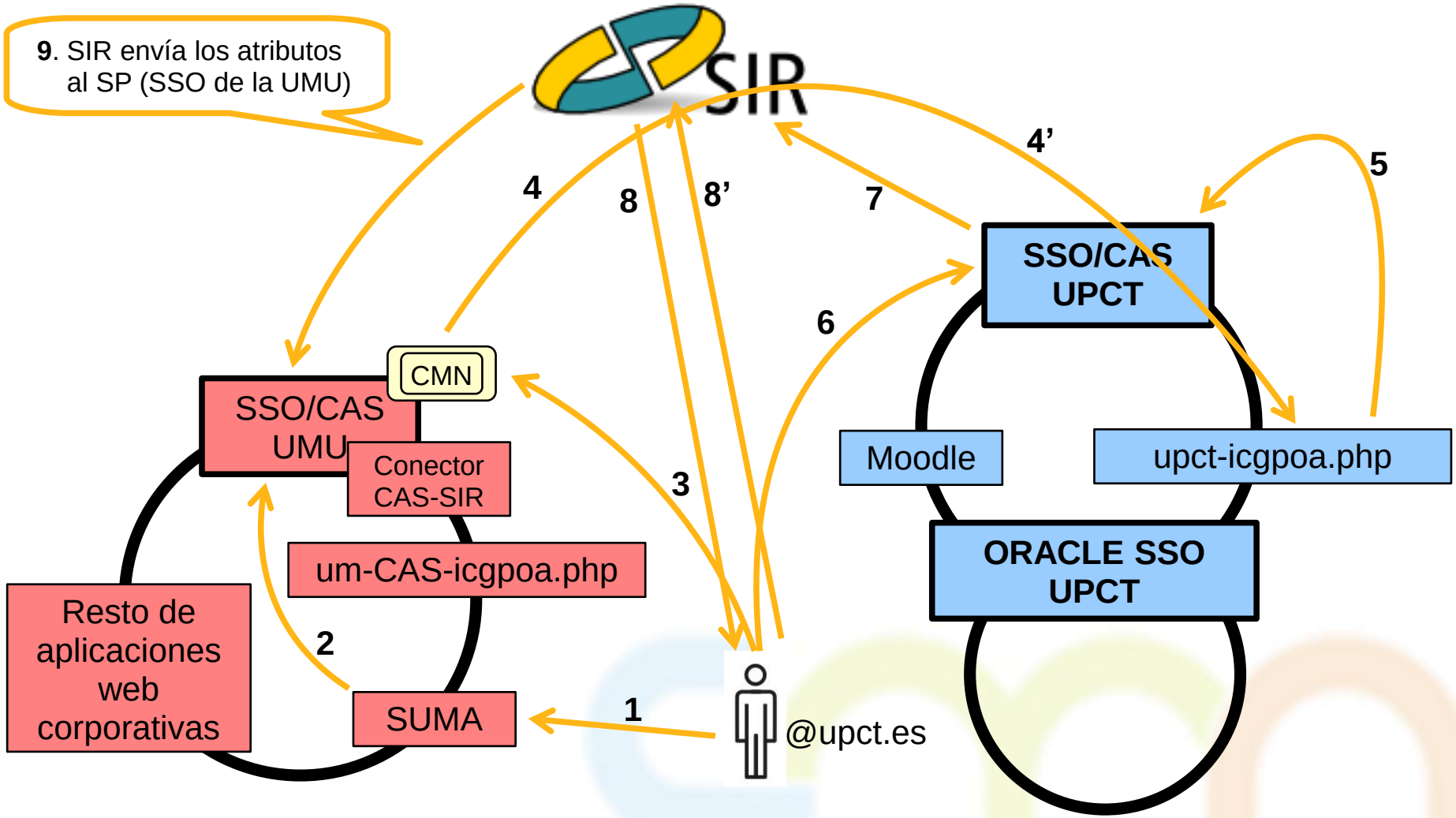
9. Ejemplo de uso de la Federación CMN



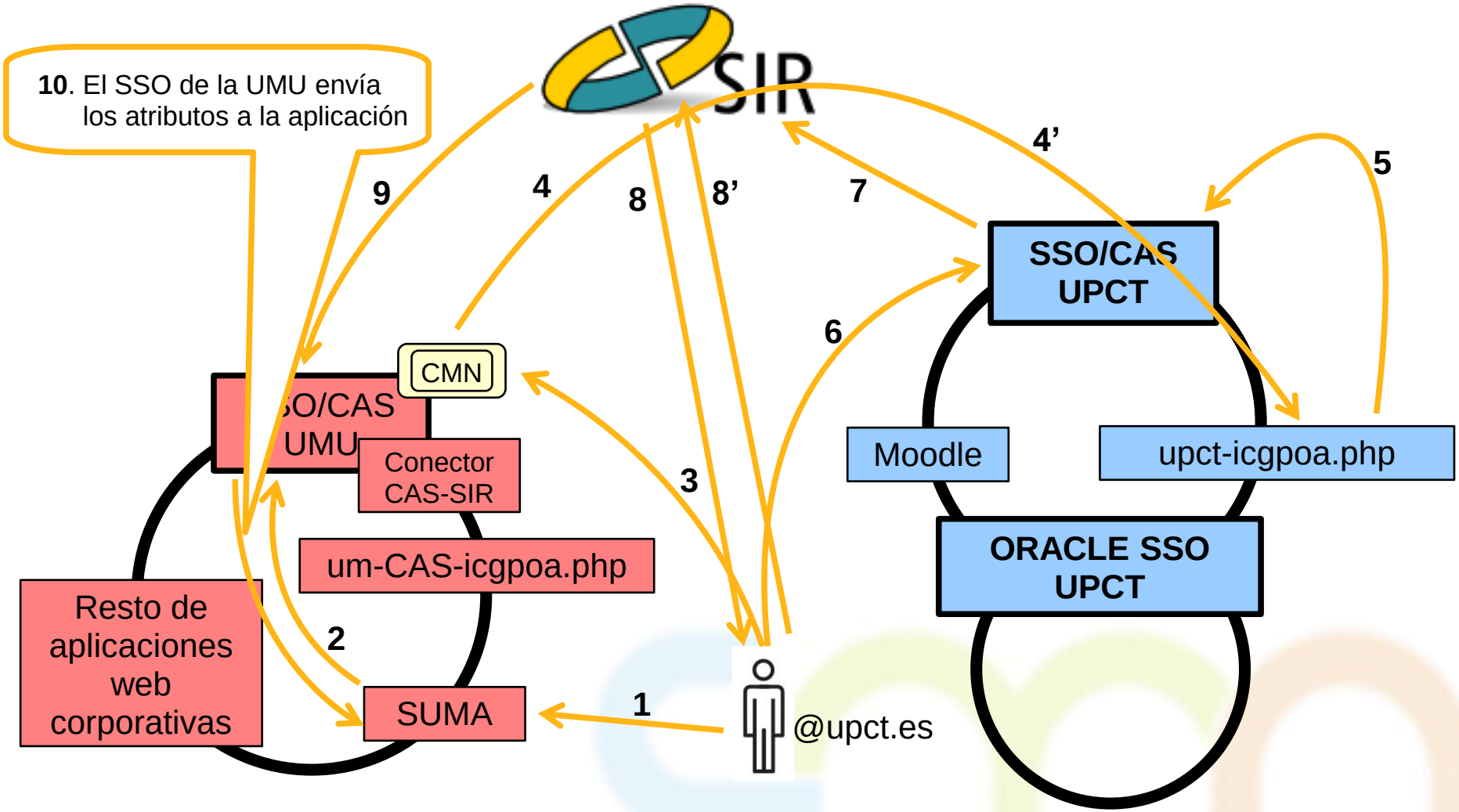
9. Ejemplo de uso de la Federación CMN



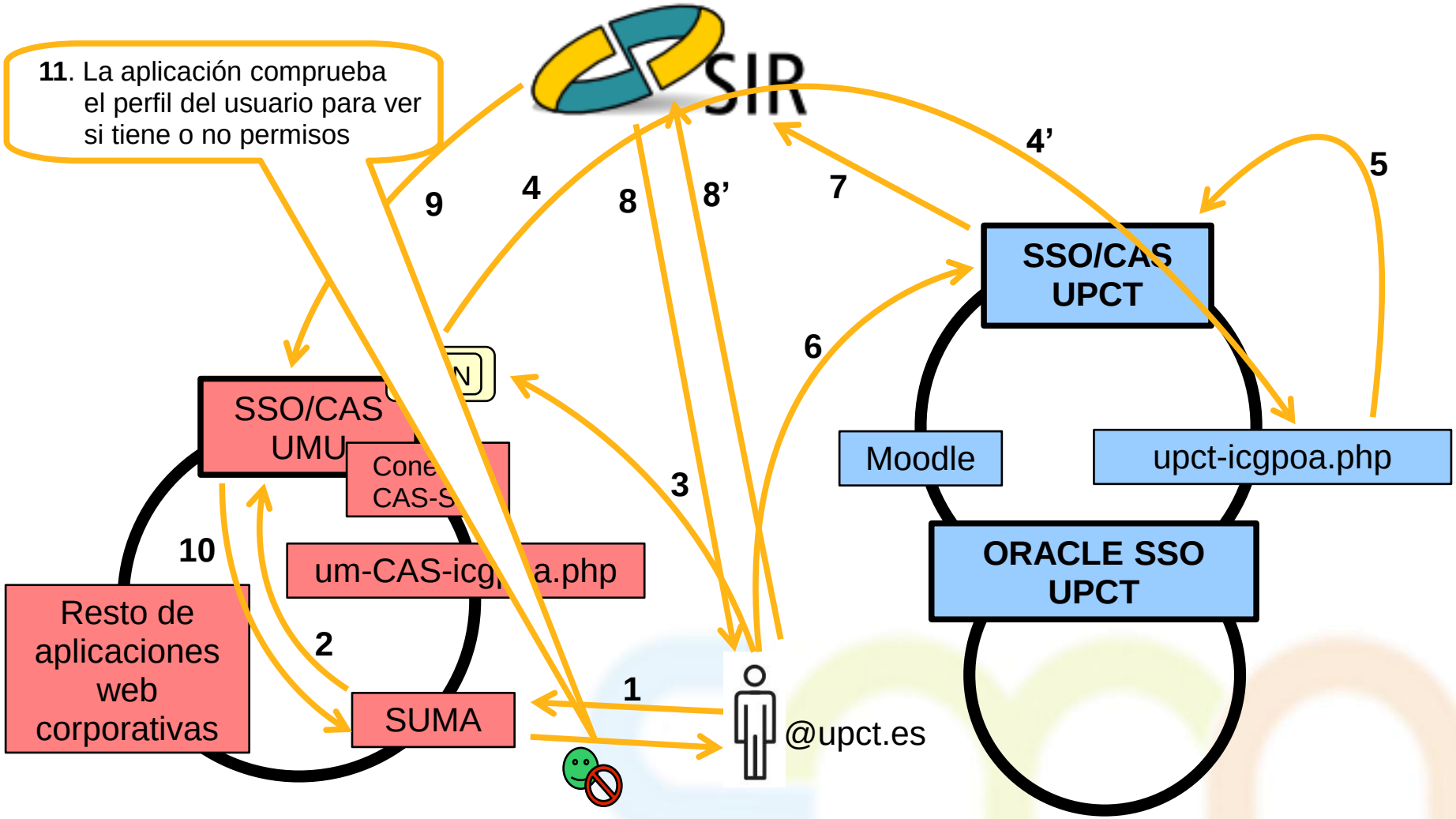
9. Ejemplo de uso de la Federación CMN



9. Ejemplo de uso de la Federación CMN



9. Ejemplo de uso de la Federación CMN



Demostración de la conexión SIR - CMN

10.- Futuro

10. Futuro

- Puesta en marcha de la federación (con aplicaciones reales).
- Fijación y normalización de atributos SIR.* a intercambiar entre la UPCT y la UMU.
- Filtrado de atributos SIR.* según aplicación del SP (en el CAS).
- Uso de certificados digitales.
- Conexión a otros sistemas de autenticación y autorización federados (OpenID, Live@EDU, ...).

11.- Enlaces de Interés

11. Enlaces de Interés

- Campus Mare Nostrum: http://www.**campusmarenostrum**.com
- Servicio de Identidiad 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**/