



## IRIS-middleware Productos en cartera



Red  
IRIS

red.es



- **Registro de URNs bajo urn:mace:rediris.es**
  - <http://www.rediris.es/si/urn/>
  - Formalizado de acuerdo a los requisitos de MACE
  - Dos organizaciones (UNILEON y UMA) registradas
  - Espacios para COPA y esquemas LDAP
- **Repositorio esquemas iris-ldap**
  - <http://www.rediris.es/ldap/esquemas/>
  - COPA y CATRE 1.0.8
    - Aplicaciones COPA en varios centros (UNILEON, UMA, UNED?....)
  - Esquema para IRISGrid
- Demostración de las tecnologías CATRE y COPA en dos portales:
  - <http://rtr.rediris.es/> (Clasificación colaborativa de recursos)
  - <http://irisgrid.rediris.es/vosnav> (Gestión de VOs en IRISGrid)
- Clases irisPerson, irisInetEntity, irisObject
- Esquemas PAPI

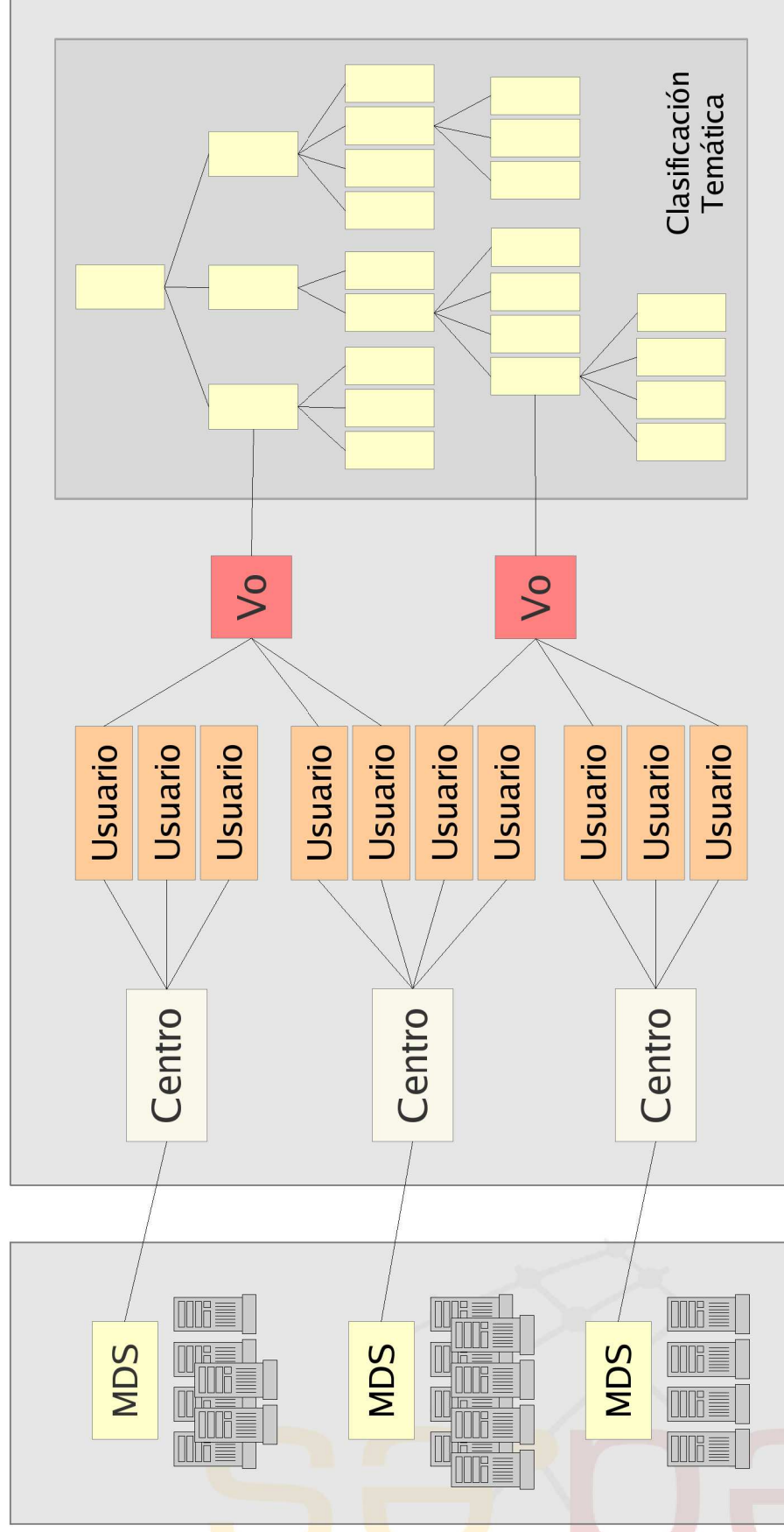


- Nuevos atributos guiados por la experiencia real en instituciones
  - irisPersonalUniqueID
    - Identificador único (DNI, NRP,...)
    - Posibilidades de hacerlo opaco
  - irisUserEntitlement
    - Modelado de derechos
    - Permisos intra- o inter-institucionales
  - irisUserPrivateAttribute
    - Denegación de acceso a ciertos datos
    - Definible por el usuario, compatible LOPD
    - Gestionado a nivel del propio servidor LDAP
- A través de la lista IRIS-LDAP



- Propuesta para crear un comité para el expansión del esquema
  - Participantes: UMA, UPO, UNILEON, CSIC,...
- Más sobre su aplicación a medida que ganemos experiencia
  - Escalabilidad
  - Usabilidad
- **Coordinación internacional**
  - Con la TF-EMC2 y el MACE de Internet2
  - Propuesta para mantener un registro de esquemas
    - <http://www.daasi.de/services/SchemaReg/>
  - El objetivo es la armonización internacional
  - Permitiendo el intercambio de datos
    - Y siempre tendremos irisUserPrivateAttribute!





Recursos IRISGrid

Directorio IRISGrid



- **Significativas mejoras en modo proxy**
- Transferencia en chunks (*Proxy\_Chunk\_Size*)
- Proxy HTTPS con *Remote\_URL* y *Remote\_Domain*
- Gestión de cookies con path explícito con *Remote\_Domain*
- Manejo de eventos JavaScript (marcas *onXX*)
- Buena parte de ellas, producto de contribuciones de usuarios del software
- UCO, UNED, TSM
- Soporte a través del portal PAPI
- <http://papi.rediris.es/comu/proxies/>
- Actualización automática en estudio
- El RewritingProxy PAPI constituye una alternativa a cualquier sistema de proxy de aplicación HTTP
- Wok es un ejemplo paradigmático

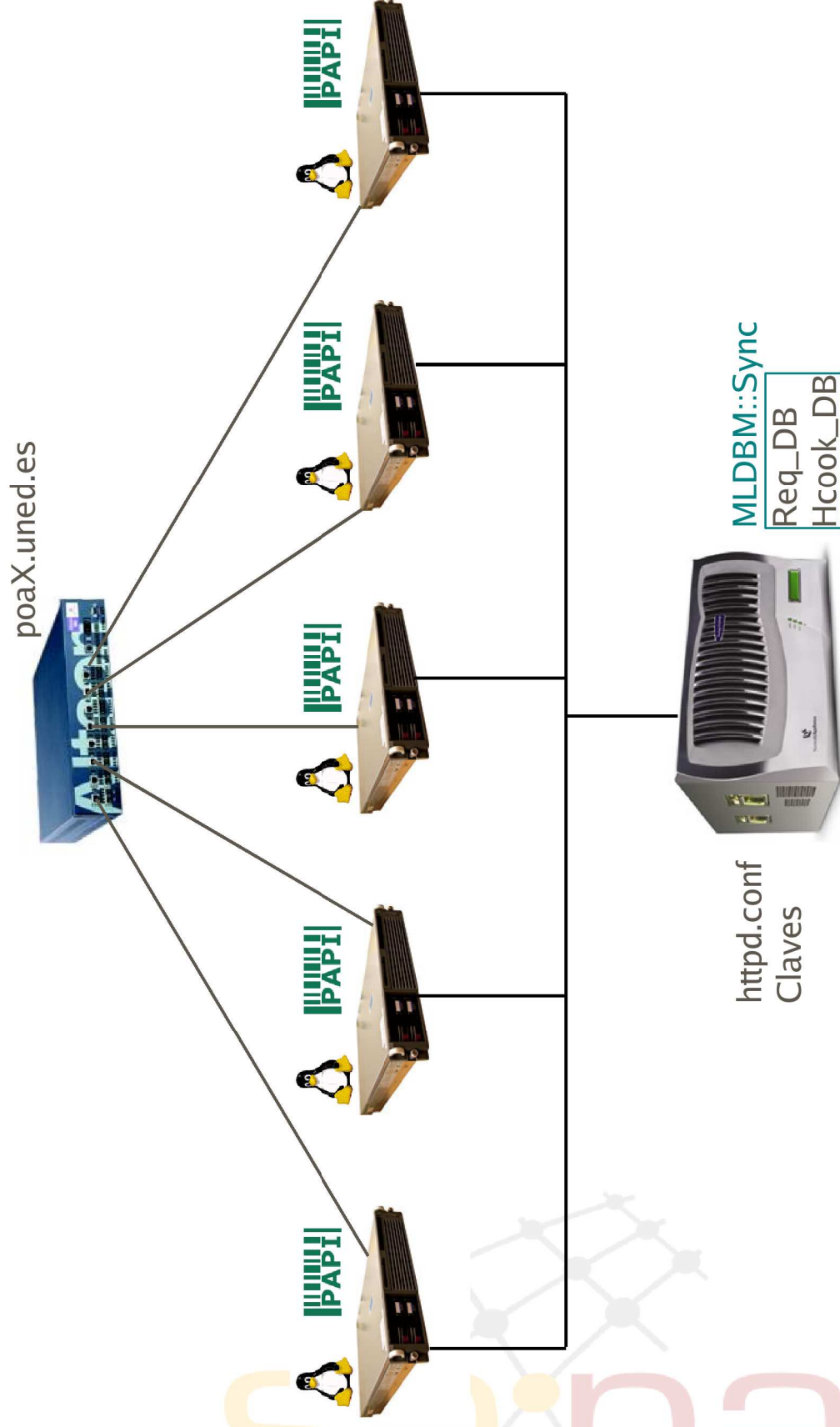


- Basada en un fichero XML independiente
- Independiente del sistema de configuración de Apache
- Compatible con cualquier agrupamiento de los URLs
  - *Location, Directory, File,...*
  - Extensible a otros servicios
  - Multiplataforma
- **Ha posibilitado el desarrollo de una aplicación de gestión**
  - Interface web
  - Diferentes niveles de configuración
  - Ayuda on-line
  - Integrable con el portal PAPI

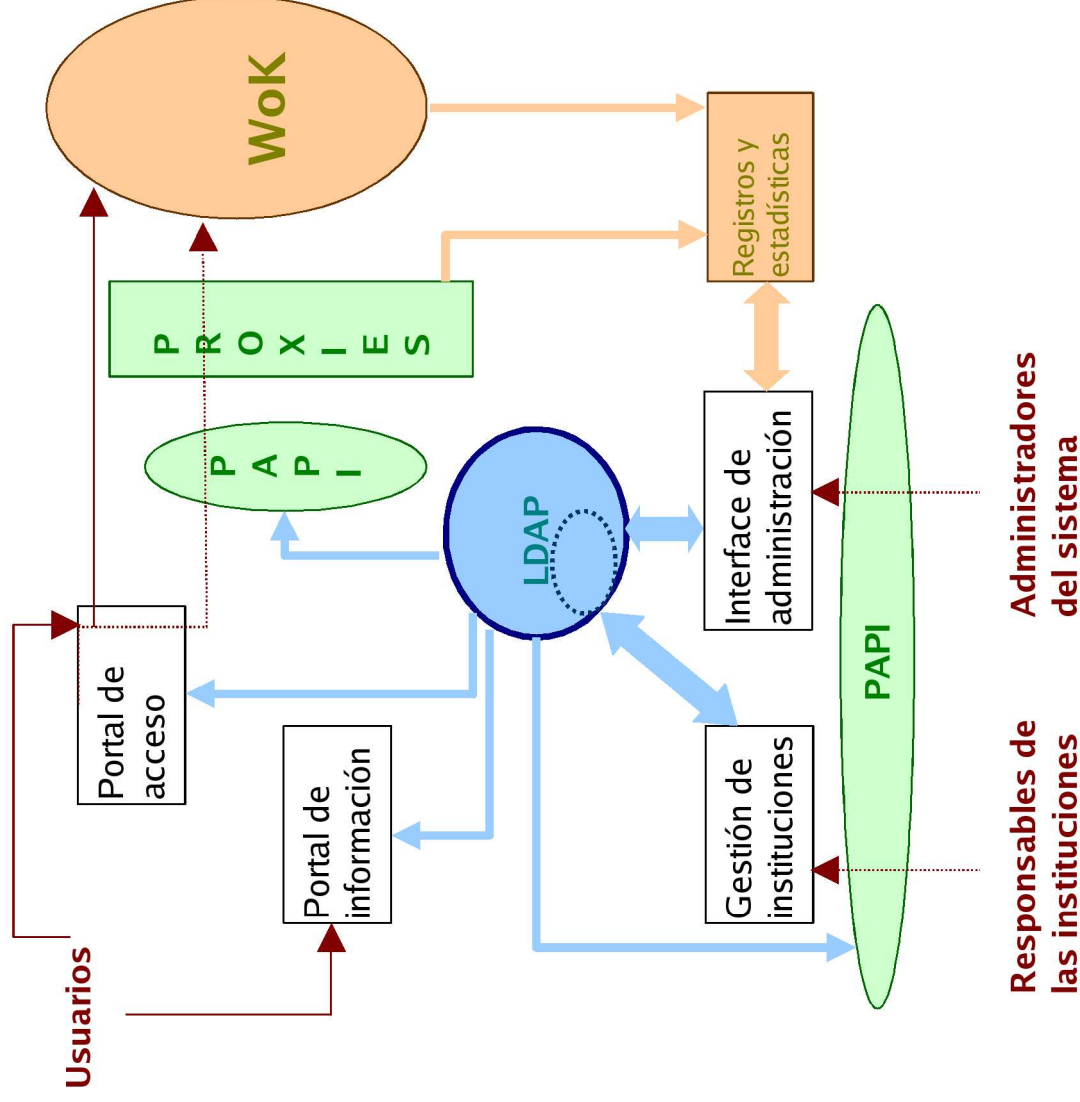


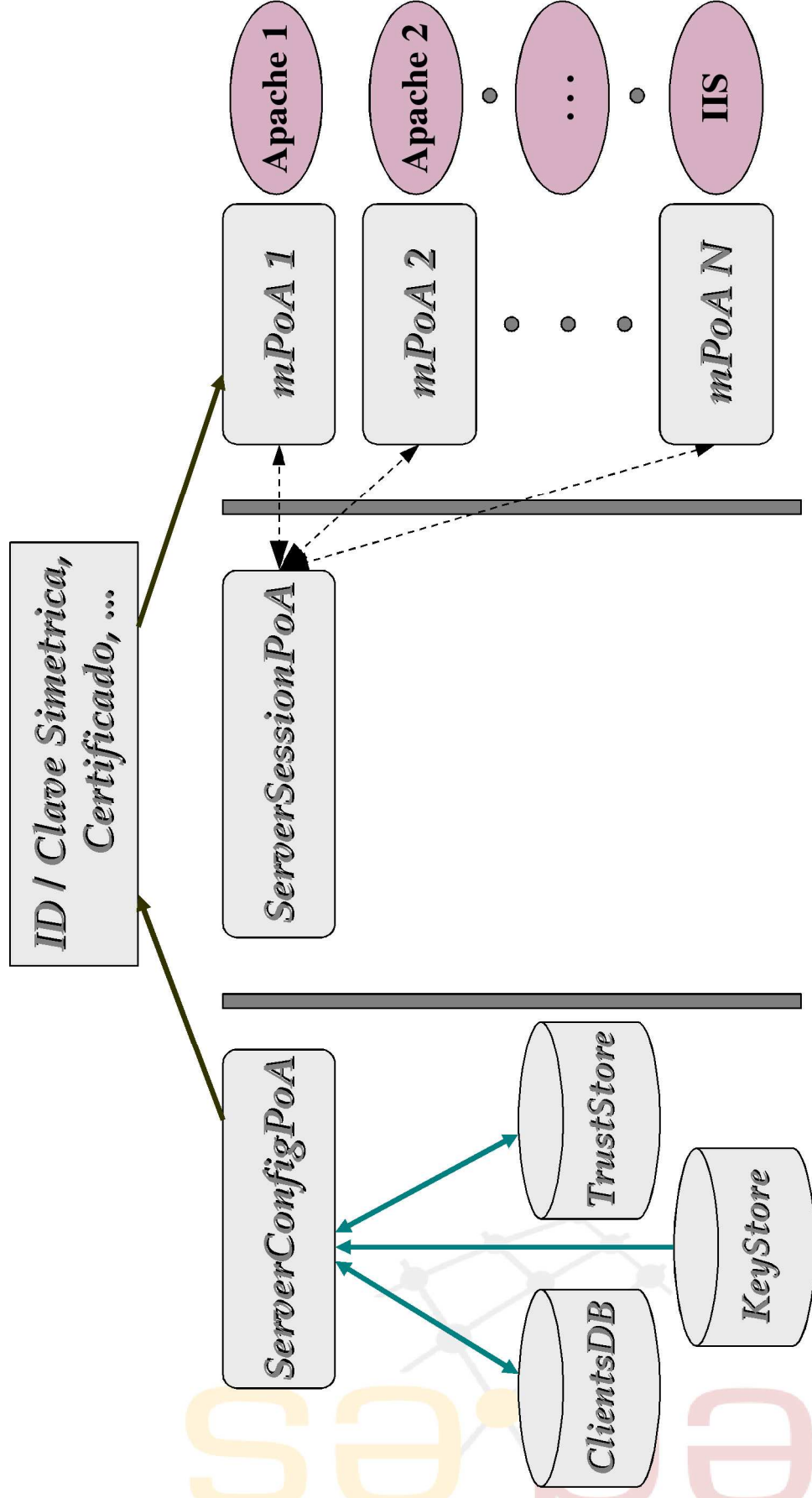
- **Finalizada la integración con JNLP**
  - Permite el arranque de aplicaciones por medio de HTTP
  - Base de la arquitectura Java WebStart de Sun
  - Colaboración con el CIEMAT
  - Extiende SSO a aplicaciones accesibles a través de la Web
- **Finalizada la conexión PAPI/Athens**
  - Posibilidad de acceso a recursos de biblioteca sin proxy
- **Prototipo de PoA con variables locales del servidor**
  - Aplicaciones como WebCT
- **Primeros experimentos con RTSP**
  - Acceso a contenidos multimedia
- **Otros frentes**
  - Sympa, Oracle SSO (software OCU), Kerberos



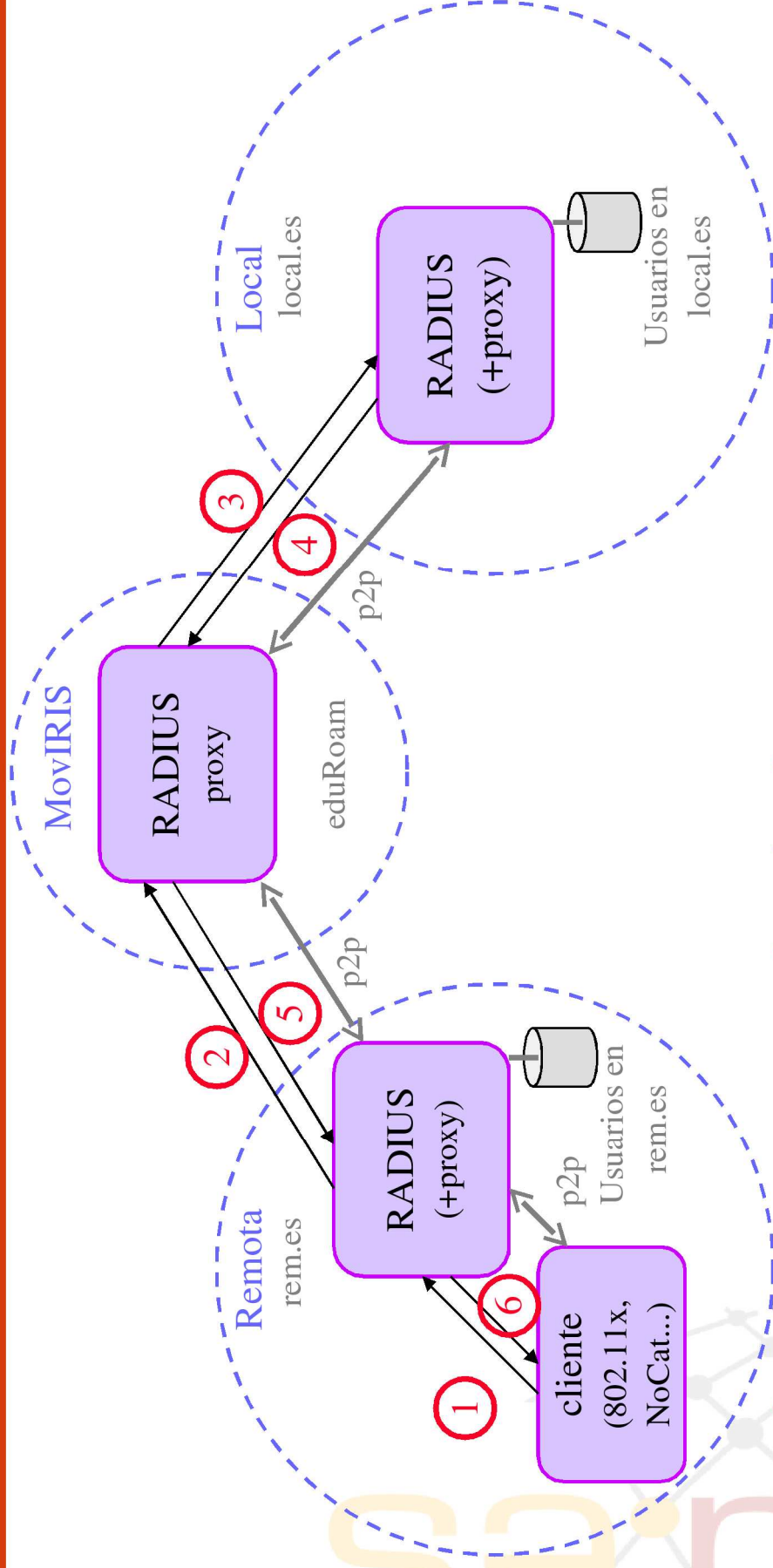








- Creación del entorno de colaboración
  - Soporte (páginas web, listas, etc.)
  - Política de acceso a nivel nacional
- Contactos con organizaciones en proceso de sumarse a la iniciativa: CESCO, CSIC, FUNDECI, UC3M, UCLM, UDC, UGR, UM, UNED, UNIZAR, UPM
- Asociados al espacio de movilidad europeo (eduRoam)
- Entorno capaz de integrar los tres métodos de acceso compatibles eduRoam
  - 802.1x, Web, VPN
- Primeros pasos en la integración con otros sistemas de control de acceso
- Colaborando con las iniciativas de la TF-Mobility



- **Confianza por intercambio de claves**

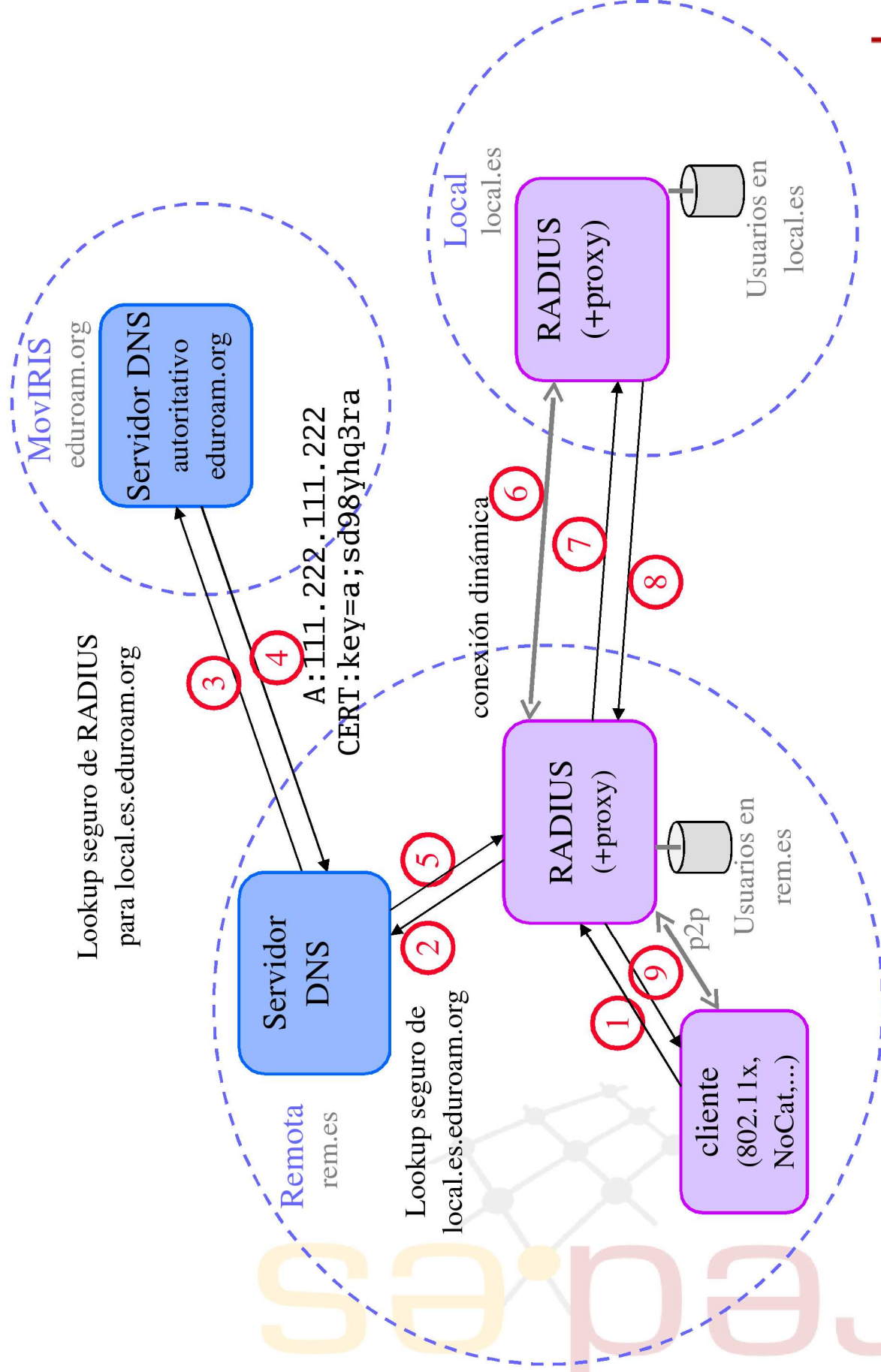
- **Experimentos proyectados para el uso de una PKI**

- **Alternativas en discusión**

- **DIAMETER (poco probado y con dudas acerca de su despliegue)**

- **DNSsec**







- **RedIRIS Weathermap**
  - <http://www.rediris.es/red/ri2wm/>
  - Emplea XML como formato intermedio para representar los datos
  - Aplicación Java extensible a otros dominios
- **DetectIRIS**
  - Servicio para la detección por usuarios finales y administradores de características y problemas en la red
  - Los test actuales detectan: filtros, ancho de banda disponible en TCP y UDP, soporte multicast, soporte IPv6, ...
  - Basado en portal, servidores y cliente
  - Más sobre esto en breve

- **TERENA Academic CA Repository**
  - <http://www.tacar.org/>
- Una fuente fiable de certificados raíz y política
- **El repositorio se construye y actualiza por medios fuera de banda**
  - Encuentros personales con los oficiales de TERENA
    - Actúan como fuentes iniciales de confianza
    - Esenciales para la incorporación inicial
  - Correo basado en PGP
- **Accesos alternativos a los certificados**
  - HTTP(S)
  - PKCS#7
  - LDAP

- **La política ha sido aprobada**
  - Incluye documentos de muestra
    - Qué PKIs pueden participar
    - Cómo incluir, modificar y distribuir los datos
    - Procedimientos para cambiar la propia política
- **Se están incorporando PKIs**
  - 17 (+2 en espera)
    - CASNRENS y autoridades Grid
  - **Relación directa con la EUGridPMA**
  - **Buscando nuevos campos de aplicación**
    - Soporte del eIRG (junto con la EUGridPMA)
    - EGEE
    - The *Evolvable PKI* group (Internet2)

- Una fuente autoritativa única para certificados y políticas
  - Que simplifique las labores de mantenimiento
- Un mecanismo para extender (y reforzar) los vínculos de confianza
  - Comunidades grid
  - Otras áreas geográficas
- Un modelo con el que experimentar
  - Distribución de certificados empaquetados
  - Modelos basados en *peer reviews*
    - Cualificados o no
  - Bridges y modelos similares
    - Integración con el modelo XPS
  - Servidores externos de operaciones de PKI
    - Simplificación de la evaluación de confianza





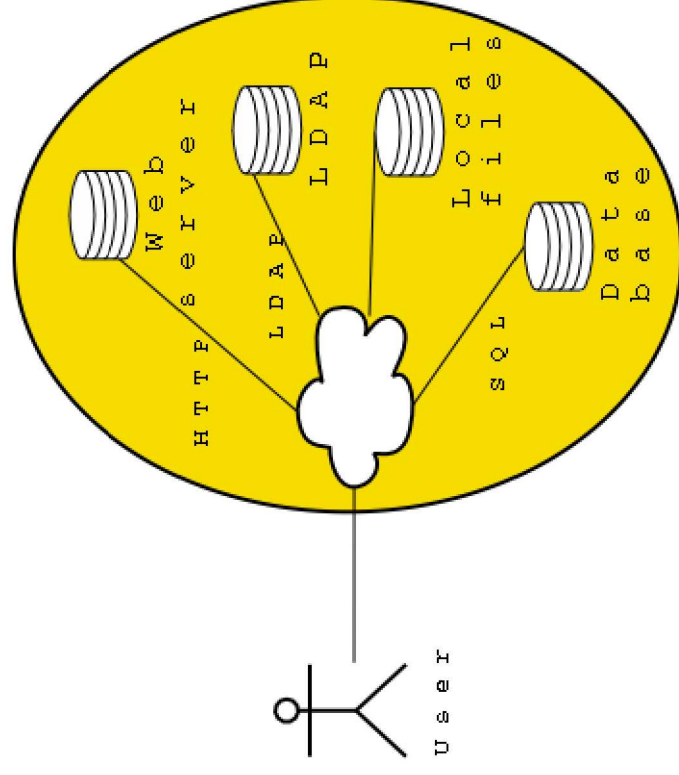
- **Aceptación automática de certificados de servidor por los browsers**
  - Coordinado para todas las NRENS europeas
    - Ahorro de costes
- **Las NRENS operarían RAs de este servicio**
  - Con posibilidad de delegar el registro en las instituciones
- **Dos alternativas**
  - Proceso de aceptación de los fabricantes
  - Externalización con un proveedor
- **Reunión para fijar políticas (3 de noviembre)**
  - Estructura de costes y delegación
  - Especificaciones de la externalización
  - Reportar interés en cada una de las comunidades

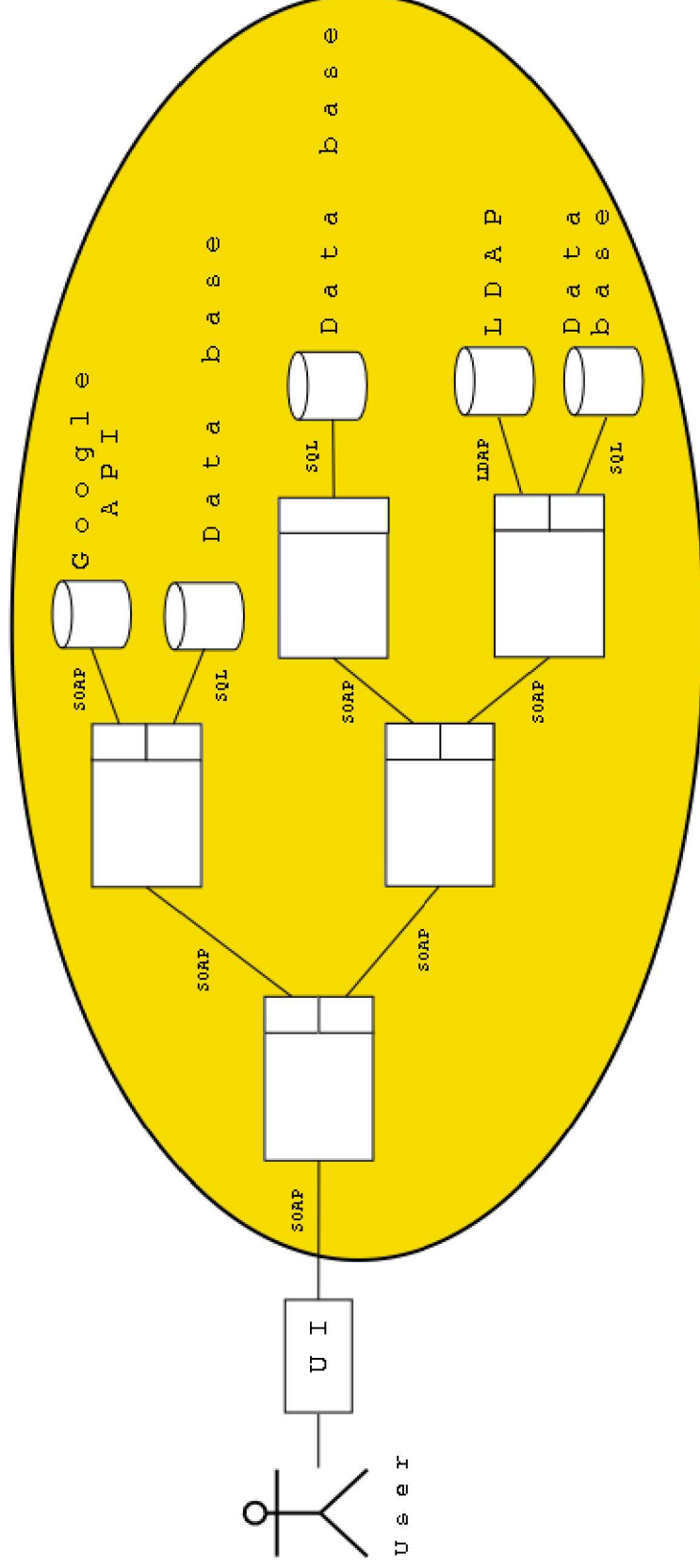


- Una capa de abstracción para integrar sistemas de búsqueda
- Integración de APIs: federación de servicios -> SOAP + HTTP
- Modelo semántico: integración de datos -> RDF + Dublin Core

### • Con capacidad de ser

- Escalable
- Extensible
- Simple de configurar
- **Propuesta SOLFA**
- Federación de forjas académicas
- Docencia-NET





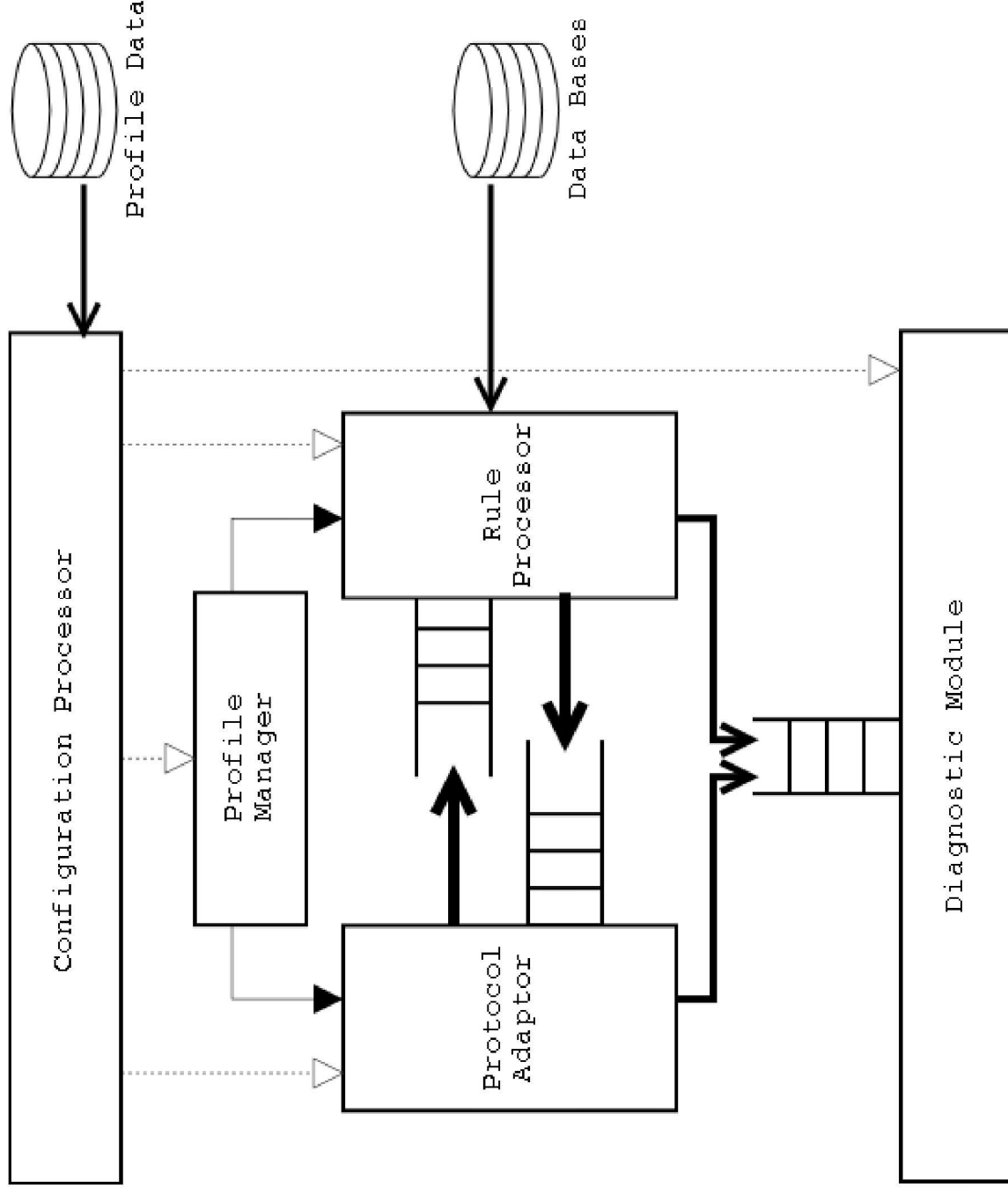
- Cada fuente incorpora un agente, accesible por SOAP
- Las consultas y respuestas emplean RDF con un vocabulario Dublin Core
- Agentes para LDAP, SQL, el API Google y Searchy

- Movilidad e infraestructuras de AA
- Integración de servicios: SSO global
  - Red, recursos y aplicaciones
  - RedIRIS coordina la actividad de AAI
- Propuesta de interface abierta para su uso por las otras actividades
  - JRA1 (monitorización)
  - JRA3 (BoD)
- Reaprovechamiento de resultados: AA-RR
  - Base para los módulos de interconexión
- La primera fase de los actividades de movilidad se basará en la infraestructura y resultados de eduRoam

- Una herramienta capaz de asumir el papel de cualquier componente en una AAI
- *Attribute sources (AS)*: Aceptan preguntas y responden con atributos de usuarios y aplicaciones
- *Attribute requesters (AR)*: Realizan peticiones a los AS y las procesas, usando en algunos casos los AE
- *Authorization engines (AE)*: Responden las peticiones de los AR aplicando reglas internas de autorización (*políticas*)
- **Controlada por perfiles**
  - Comportamiento
    - Entidades
    - Cuestiones de protocolo
  - Atributos y valores
- **Neutral frente a protocolos**
  - SAML/XACML, SPOCP, RADIUS



- **Versión actual**
- Configuración XML
- Adaptador de protocolo SAML
- **Demostrado en la última reunión de la JRA5**
- **Colaboración con FUNET y Sun**





- Una reunión entre grupos internacionales y los que se baten *el cobre en los campus*
- Intercambio bidireccional: Oferta y demanda en middleware
- Eminentemente práctico
- Buscando la colaboración de EUNIS
- **Planteado en tres días**
- Identidad digital (directorios, privacidad, armonización,...)
- AA (tecnologías, integración en las aplicaciones,...)
- AA en el acceso a la red (802.1x, VPNs, trazabilidad,...)
- **A primeros de marzo de 2005**
- Unas 100 plazas
- Lugar: Las Palmas o alguna ciudad italiana
- **Programa definitivo a primeros de noviembre**

- Organizado por el JISC
- Países que disponen de software y servicios para AAI
  - Australia, Finlandia, Holanda, Suiza, USA, UK, España (+ CERN)
- Facilitar la interoperabilidad de infraestructuras de AA
- En proceso de constitución
- Primeros objetivos
  - *The Slaughter Recipe*: Cómo constituir una AAI de acuerdo a unas normas mínimas
  - Constituir un grupo de confianza similar a la EuGridPMA
  - Fuentes de financiación
    - NRENs participantes
    - CE y otros organismos internacionales
- Directamente relacionado con propuestas en España
  - FedIRIS
  - Iniciativa sobre e-ciencia