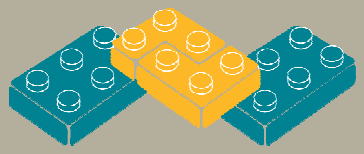
Red IRIS

PAPI
Nuevo software
Nuevos servicios



middleware

Madrid, 9 de mayo de 2003

Índice

- La nueva versión de PAPI: 1.2.1
- Próximas versiones
- PAPI@RedIRIS
- Quién usa PAPI
  - Propuesta de interconexión Athens
- PAPI y otros métodos de control de acceso

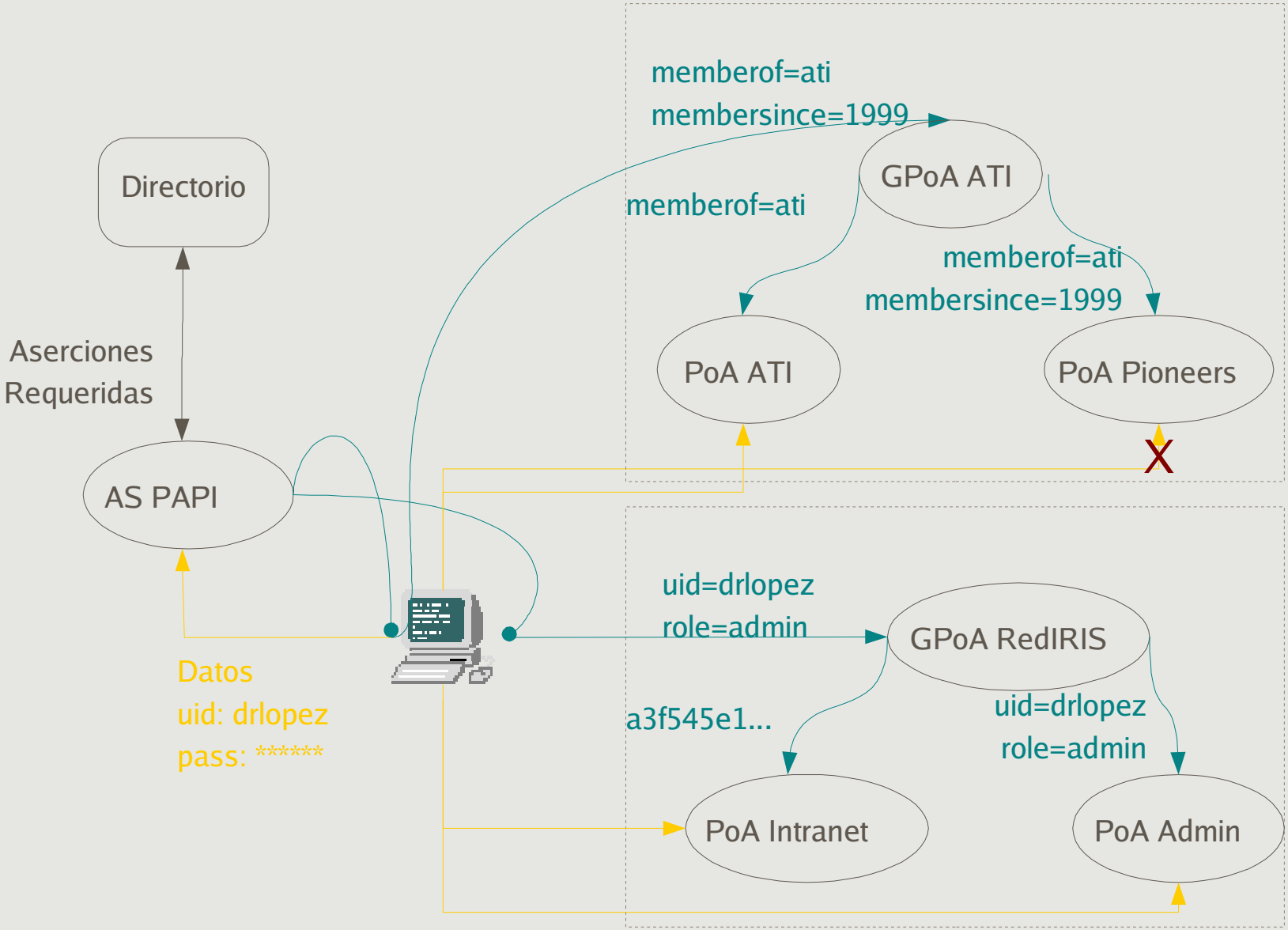
PAPI 1.2.1 - Principales características

- Mejor soporte para autorización basada en atributos
  - El AS puede enviar aserciones individualizadas
  - El PoA tiene un mejor control sobre los datos en estas aserciones
- Mejores mecanismos de personalización
  - Objetos específicos de aceptación/rechazo
  - Redirección automática en el AS
- Modo proxy más completo
  - Aplicable a un dominio completo
  - Soporte de autenticación HTTP
  - Desacoplo origen/destino

Autorización basada en atributos

- Para cada (G)PoA al que enviar datos sobre un usuario se deriva un formato de aserción
  - Datos del propio usuario
  - Definición del (G)PoA
  - Valores por defecto en el AS
- En el formato pueden emplearse
  - Variables de conexión
    - Username (o un hash), una nonce, datos recibidos a través de los forms HTML o la configuración
  - Atributos del usuario
    - Basado en LDAP, aunque otras fuentes también son aplicables

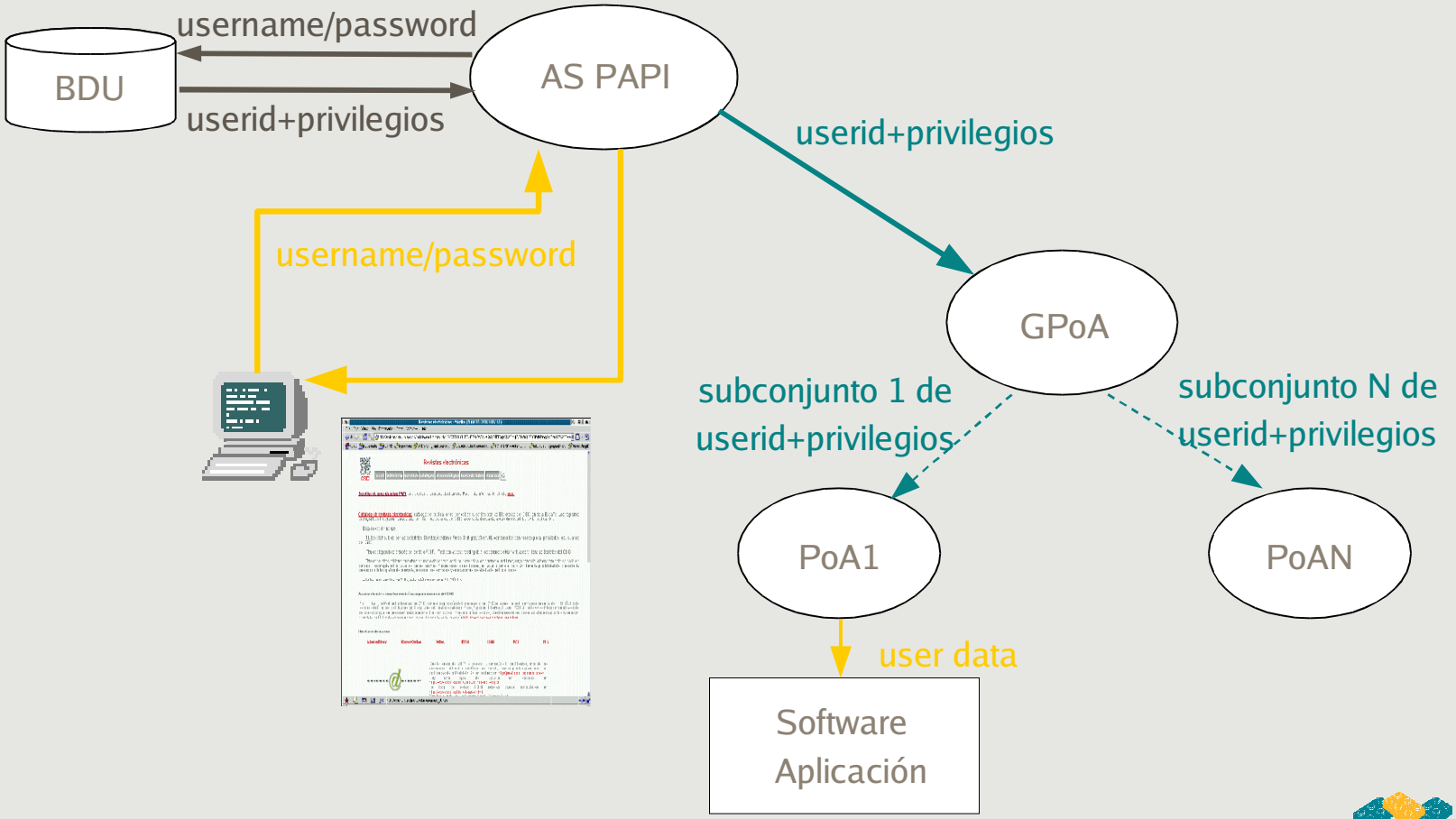
Autorización basada en atributos



Mejor personalización

- Uno de los puntos fuertes de PAPI
  - Soporte para una *identidad digital*
  - Portales con acceso a servicios in-/externos
  - Compatible con la privacidad del usuario
- Capacidades de personalización
  - Los objetos requeridos a los PoAs en la primera conexión pueden ser específicos de cada sitio.
    - Experiencias con JavaScript y CSS
  - Las aserciones se pueden usar para transmitir datos a las aplicaciones (`Hcook_Handler`)
    - Experiencias con CGIs, PHP, JSP, MetaFrame,...
- Mucho que experimentar

Personalización basada en atributos



Modo proxy

- Es una respuesta de sentido común al problema del huevo y la gallina
  - Ningún proveedor soporta una tecnología insuficientemente implantada
  - Nadie la adopta si los proveedores no la soportan
  - Las mejoras están motivadas por el uso diario
- Soporte de autenticación HTTP (Basic y Digest)
  - En el futuro usará los contenidos de las aserciones => mejor personalización
  - Experimentos con autenticación basada en forms
- Soporte proxy para un dominio completo
  - `poa.papi/srv/loc -> srv.rem.dom/loc`

Próximas versiones: PAPI 1.3

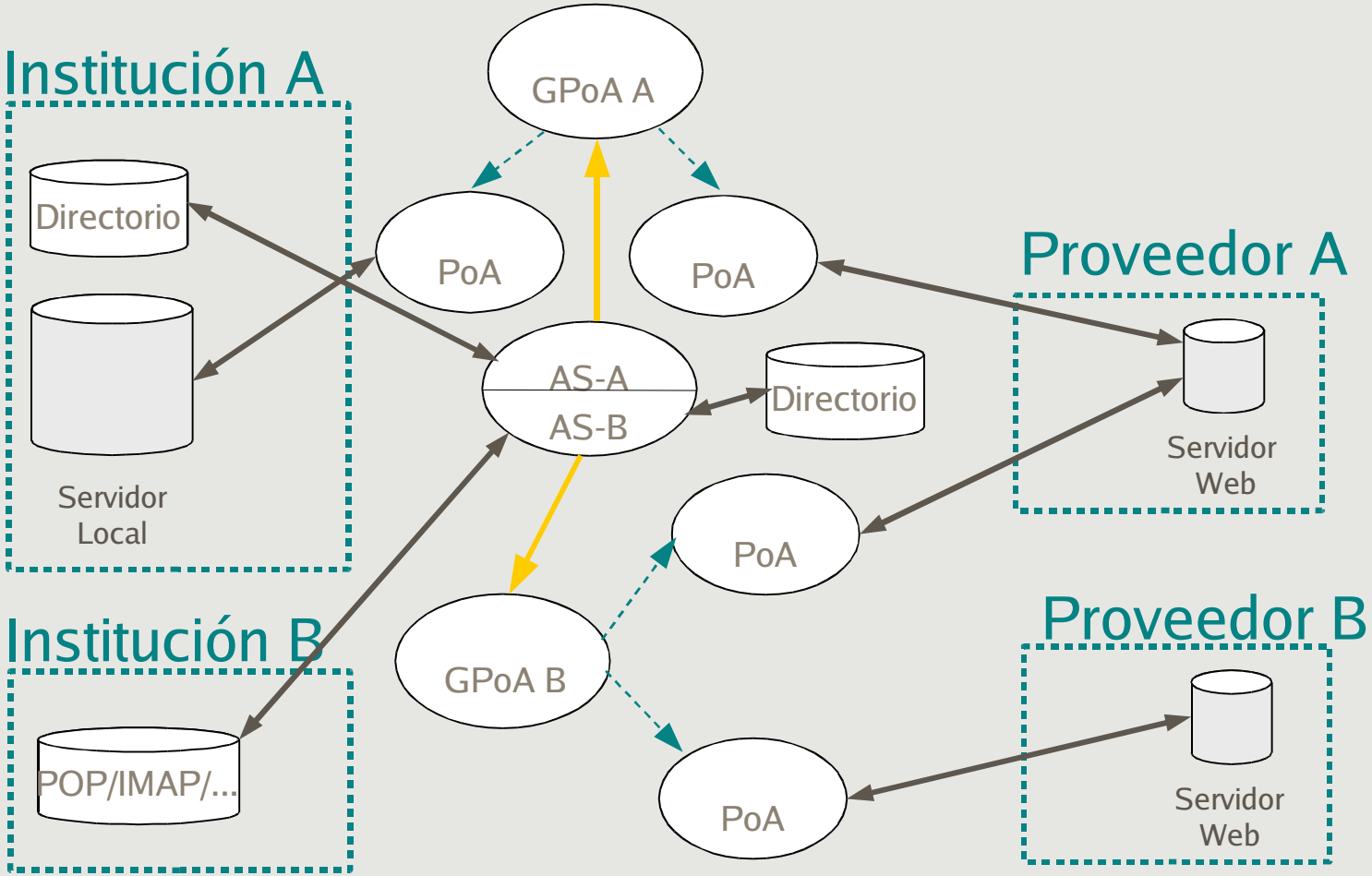
- Prácticamente compatible con PAPI 1.2
- Uso de SPOCP como motor de autorización
  - Control de acceso mucho más fino
  - Deslocalización de las políticas de autorización
- Interrogación directa PoA/AS
  - Evita la necesidad de la conexión inicial
  - Integración con otros sistemas
- Autenticación basada en certificados
- Incorporación de un motor de localización
  - Integración de PAPI con portales
- Librería de definiciones proxy

Próximas versiones: PAPI2

- Rediseño del sistema
  - Basado en Java
  - Incorporación de estándares de PMI
  - Interfaces de administración
- Propuesta de interconexión PAPI/PERMIS
  - Uso de *trusted objects* almacenados en el Directorio
  - Lenguaje de especificación de privilegios basado en XML
- Propuesta de integración PAPI/VirtualHome
  - Presentada al VI Programa Marco
  - Gestión de identidades digitales

PAPI@RedIRIS

- Facilitar la diseminación de la tecnología



PAPI@RedIRIS - Qué proporciona

- Tantos GPoA/PoA como sea necesario
  - En el dominio de la institución, o en papi.rediris.es
- Control local del interface de usuario
- Posibilidad de emplear:
  - El directorio de RedIRIS para gestión de usuarios
  - Un motor de autorización con reglas propias
  - En el futuro, un motor de localización
- Interfaces Web para el control de los elementos opcionales mencionados
  - Protegidos con PAPI
- Estadísticas de uso

Quién usa PAPI - España

- Bibliotecas
  - Con PAPI@RedIRIS: CSIC, EHU, UPC (piloto)
  - Instalación propia: CICA, US, UPO, UPC (prox)
  - Presentación a REBIUN
    - Convocatoria MECD para bibliotecas (Diciembre)
- CIEMAT: Acceso a equipamiento científico
- Contactos con otras universidades para su implantación: URJC, UNED, UPSA,...
- Los propios servidores de RedIRIS
- Contactos con la Administración

Quién usa PAPI - Fuera de España

- Redes académicas europeas
  - JISC - Proyecto GLAM
  - SURFnet - Interconexión con A-Select
  - UNINETT - Soporte para FEIDE
- Redes académicas latinoamericanas
  - REUNA está implantando un piloto
- Universidades y centros europeos
  - Oslo, Edimburgo, ZIB-Berlin
- Contactos con la comunidad Grid y el equipo de VRVS

Interoperabilidad Athens

- Propuesta por EduServ, la entidad que gestiona el sistema Athens
- Implica el acceso automático a recursos que reconocen el control de acceso Athens
  - Por medio de ASes/PoAs PAPI
  - Sin necesidad de proxies
- Permite sacar ventaja de la comunidad de usuarios Athens
- Si existe interés, RedIRIS está dispuesta a desarrollar el software de interface y ofrecer el servicio de conexión
  - Hay que determinar el coste económico (cuotas) que requerirá EduServ

PAPI y otros métodos de acceso

- PAPI es, en esencia, un sistema de autenticación y autorización
  - Incorpora un proxy para acceso a recursos remotos
- Es posible integrar otros métodos de acceso en los procedimientos AA de PAPI
  - VPNs: La red académica holandesa (SURFnet) ha realizado experiencias con ello
  - Proxies específicos: Internet2 tiene contactos con Innovative Interfaces
    - Vamos a realizar experimentos con otros sistemas, como IRIS y EZproxy
- El uso de procedimientos estándar es una garantía de interoperabilidad

La curva de aprendizaje

- Cualquier tecnología nueva supone un aprendizaje específico
- Inicialmente puede ser más compleja que otras alternativas, pero PAPI permite:
  - Mejorar la seguridad de la red
  - Ofrecer un servicio integrado a los usuarios
  - Mantener el control de cada recurso en el lugar adecuado
  - Simplificar la gestión de situaciones *especiales*
- PAPI es software libre (licencia GPL)
  - Transferencia tecnológica automática
  - Soporte interno o por contrato con una empresa