


El proyecto CONFIA



Ernesto Revilla
erevilla@yaco.es

Jornadas sobre Identidad Digital 2010
Universidad de Sevilla
05/10/2010

- El proyecto CONFIA:
 - AUPA, 10 universidades públicas andaluzas
 - Implementación Fed.Id. SAML2
 - Aplicación inicial: CAV 
 - Muy buenos trabajos previos (gracias!)
 - Tareas:
 - Infraestructura común (gestor metadatos, idp homeless, etc.) + Conectores para los LMS
 - Implantación (IdPs, conexión a SIS, etc.)
 - Formación
 - Web de difusión
 - Tiempo: 6 meses (!)



Yaco:

- Equipo de aprox. 25 personas en total (8 se involucraron en proyecto)
- Empresa Open Source & Standards
- Filosofía: Transparencia, agilidad, flexibilidad
- Experiencia con Universidades & Junta de Andalucía
- Al principio: poca experiencia en Federación de Identidad y SAML2



- Estándar, estándar, estándar → SAML2, Atributos
- Open source, open source, open source
- State of the art
- Desafíos
 - Distribución automática de metadatos
 - Provisión de usuarios al vuelo
 - 10 (!) Universidades (con sus peculiaridades)
 - Consent
 - Tiempo!



- Hacer caso a los **expertos**



- **Transparencia**



- **Copiar lo que funciona (aka WAYF.dk)**



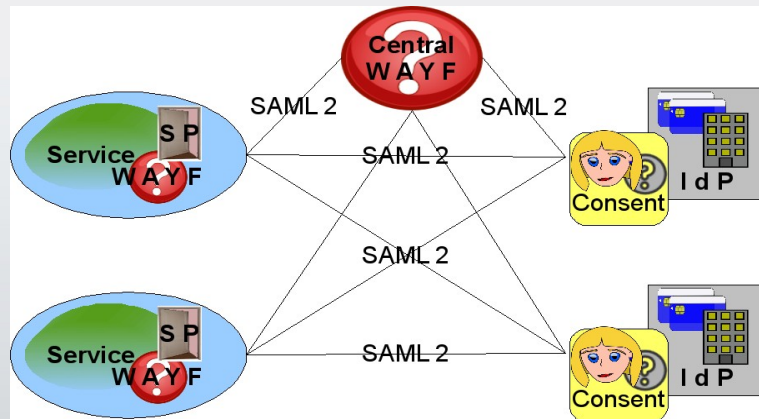
- **Colaborar (aportando granitos)**



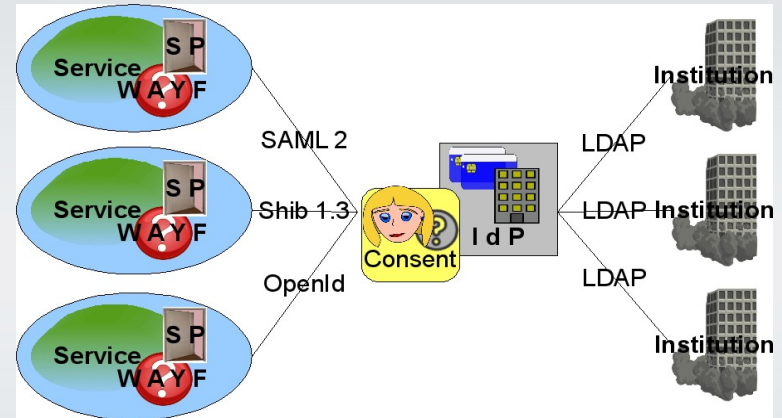
- **Transferir conocimiento**



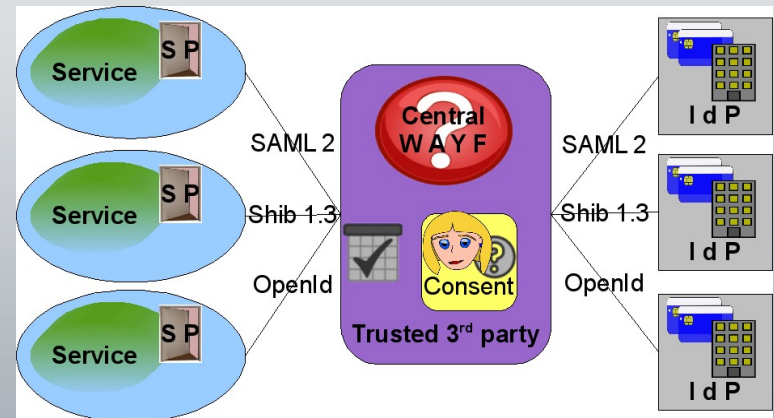
Arquitectura:



Distribuida



Centralizada



Hub & Spoke

- Esquema (conjunto de atributos):



- Software:



- Otros:
 - Provisión previa vs al vuelo
 - Directorio Virtual / Metadirectorio vs Consultas RDBMS

- **Modelo de Confianza**
 - SAML2MD y SAML2MDIOP
 - Conexiones seguras (TLS)
 - Comprobaciones de firma digital
 - Comprobaciones de las CRL
 - Actualización automática de metadatos
 - ARP



- **Protocolo: SAML2**

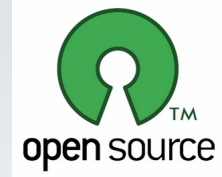
- **Arquitectura: Hub & Spoke**



- Nodo central actúa como “trusted third party”:
 - SAML Bridge
 - WAYF central
- SPs autónomos, pueden conectarse con otros IdPs y/o federaciones
- Posibilidad usar otros protocolos para SPs. (OpenId, SAML 1.1, etc.)

■ Software:

- Libertad de elección



■ Actualmente:

- IdPs usan SSP (fácil adaptar atributos)
- SPs: SSP (Moodle, BB/WebCT), Shibboleth 2.x (ILIAS).
- IdPs authentican con sistemas existentes (PAPI, OpenSSO, etc.) y obtienen datos de RDBMS (SIS)
- Filtros: crean, transforman, coleccionan y validan datos (atributos)
- SSP es fácil de escalar
- Gestor metadatos: JANUS (módulo SSP)



■ Otros (no menos importantes):

- Canal horizontal entre universidades (lista correo) & buen trabajo entre todos

- Colaboración con WAYF.DK



- Aportación código y soporte a



- CICA hospeda infraestructura común



- Web de difusión

- A tiempo !

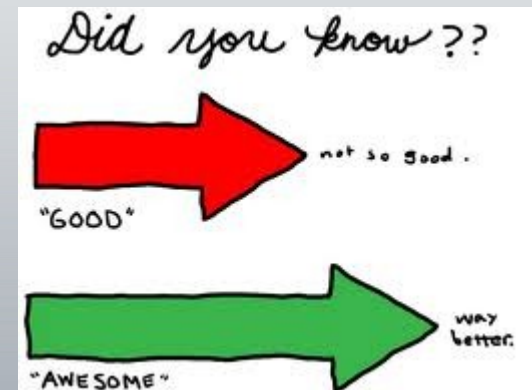


<http://confia.aupa.info>

- IdPs SAML 2.0 basado en SSP
- IdP obtienen atributos de SIS (Gestión académica)
- Consentimiento informado
- Distribución automática de metadatos (con tiempo expiración)
- Validación/verificación de certificados en gestor metadatos (CRLs / OCSP)
- Web de difusión
- Conectores para Moodle, ILIAS y WebCT con provisión al vuelo. Foodle, trac.
- Hub multiprotocolo / adaptador de protocolos
- Filtros de validación de atributos en Hub
- Módulo de autenticación X509 para SSP.



- Algunos pensamientos
 - Más aplicaciones federadas (inter & intra-universidad)
 - Integración CAU
 - Integración portal CAV
 - Optimizar validación certificados
 - Mejoras usabilidad
 - Mejoras gestor metadatos
 - Mejoras monitorización
 - Confederación (fb, google)
 - Mejoras interoperabilidad?
 - Comunicación back-channel?



¿Preguntas? ¿Comentarios?



Peter Steiner. The New Yorker, 5 julio 1993

Gracias por tu atención

erevilla@yaco.es, <http://www.yaco.es/>

