Federación de Identidades: Aproximación al Entorno Educativo

Isaac Moreno Navarro
isaac.moreno@sun.com

Arquitecto Software
Sun Microsystems

Agenda

- Introducción: conceptos básicos sobre federación de identidades
- Estándares: Liberty, SAML, WS-Federation.
- Seguridad en servicios web basados en identidad. Liberty Web Services Framework
- Federación de identidad en entornos educativos: estrategias de integración entre PAPI y OpenSSO/OpenFederation
- Sun y la comunidad educativa
- Estrategia OpenSource de Sun

Liberty e Identidad Federada

La Identidad Federada asegura la privacidad de los usuarios. Separando la **información personalmente identificable** (*PII* por su siglas en inglés), de los datos que están siendo transmitidos, conseguimos que esta *PII* sea mucho menos vulnerable, ya que si un delincuente captura una parte de los datos transmitidos, al no estar conectados a una identidad en particular, no puede hacer uso de dicha información.

Sun Microsystems , Dr. Hellmuth Broda, Distinguished Director and Chief Technology Officer, Global Government Strategy

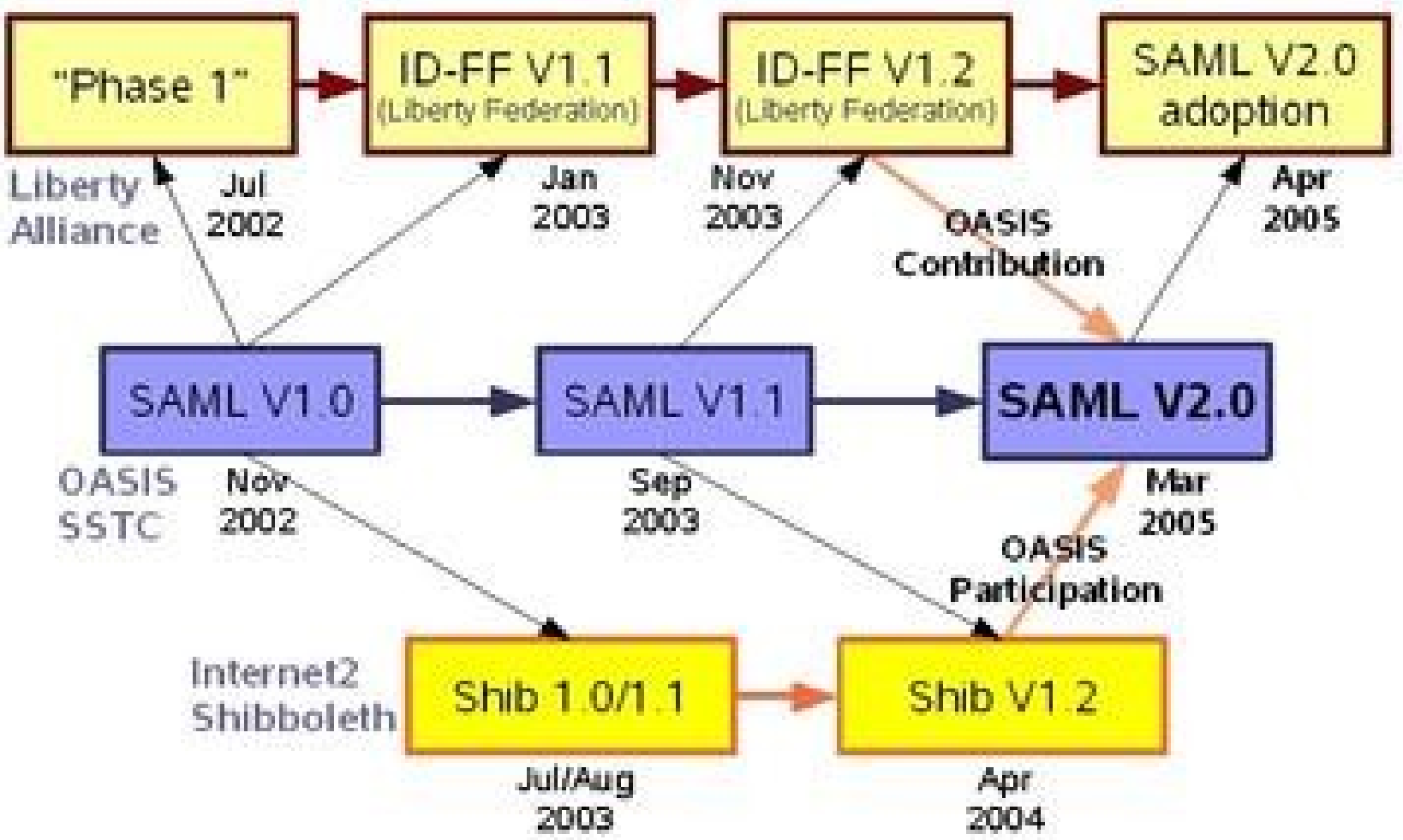
Liberty: Facilitar el desarrollo de Internet promoviendo estándares de Federación

El objetivo de Liberty Alliance es facilitar la existencia de un mundo interconectado basado en estándares abiertos donde los consumidores, los ciudadanos, las empresas y los gobiernos puedan realizar transacciones con más facilidad, al tiempo que su privacidad y la seguridad de sus datos personales queden garantizados.

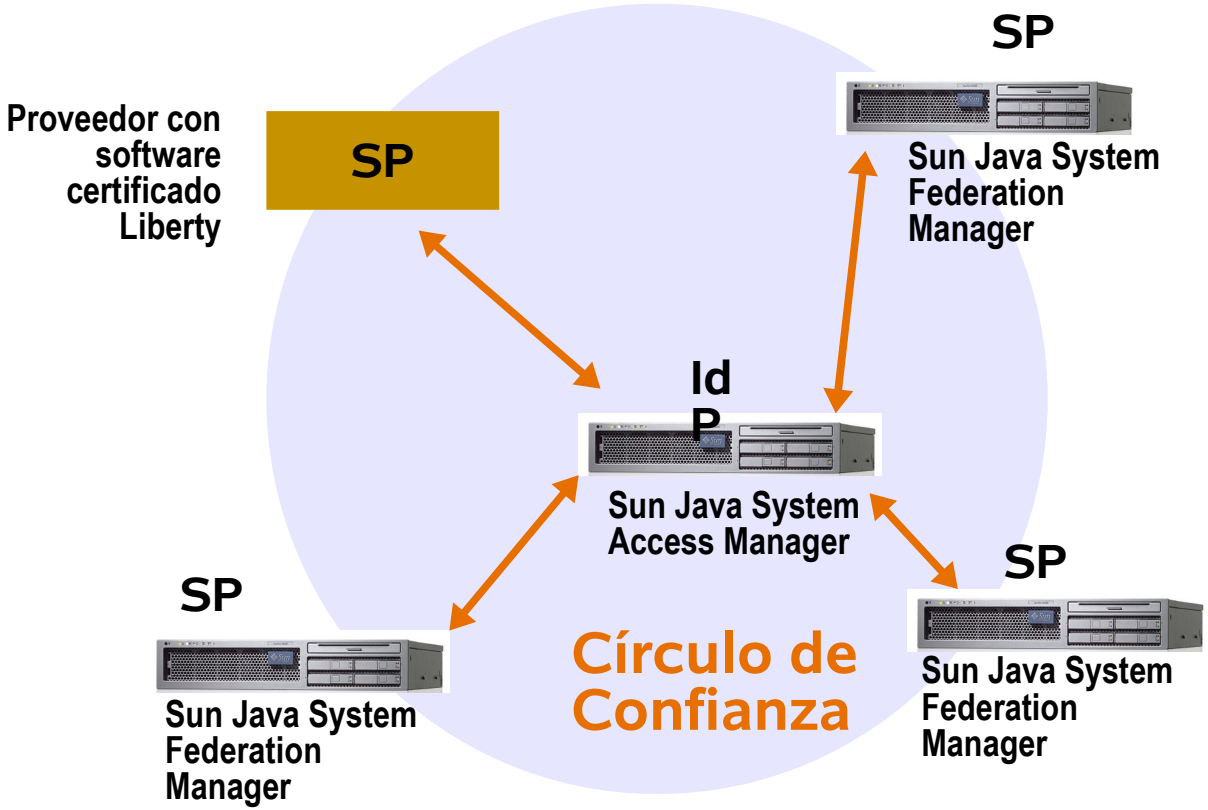
El foco principal de la alianza se centra en:

- **Construir especificaciones, basadas en estándares abiertos, para identidad federada y servicios web basados en la identidad**
- **Proporcionar soluciones contra el robo de identidad en la red**
- **Asegurar la interoperabilidad entre fabricantes y programas de certificación oficial de sus productos**
- **Colaborar con otras organizaciones de estandarización, entidades privadas y gobiernos.**

Estándares



Arquitectura básica



- Access Manager y Federation Manager permiten desplegar un Círculo de Confianza completo
- Son interoperables con cualquier otro producto certificado Liberty

Web Services Framework (I)

Liberty ha definido un marco de trabajo (framework), que soporta el desarrollo de servicios web estándar, basados en la identidad y en la identidad del consumidor, junto una serie de clientes adecuados para utilizar dichos servicios. Por tanto, es aplicable también a servicios no basados en identidad

El Identity Federation Framework (ID-FF), basado en el estándar OASIS SSTC SAML, especifica un modelo de autenticación de terceros donde los servicios individuales confían en aserciones generadas por un proveedor de identidad, por lo que el servicio no necesita autenticar directamente al usuario.

En cualquier caso, la autenticación resulta en una aserción SAML que es utilizada para comunicar el evento de autenticación a los servicios interesados.

Tipos de servicios en ID-WSF

- Estándar – No están basados en el acceso directo a datos de identidad, son de propósito general
- *Identity-based* – Proporcionan un acceso directo para la consulta y/o modificación de datos pertenecientes a un usuario concreto
- *Identity-consuming* – Hacen uso de datos asociados a una identidad para ofrecer un servicio
- Cualquiera de ellos puede implementarse siguiendo WS-I Basic Profile o disponer de un documento de descripción WSDL, por ejemplo

ID-WSF con web services estándar

- SOAP Binding – Proporciona varias cabeceras SOAP que permiten características específicas:
  - Correlación de mensajes
  - Seguridad vía WS-Security
  - Uso de políticas y directivas
  - Timeout para la ejecución del servicio
  - ...
- Mecanismos de seguridad de Liberty – Protegen los mensajes SOAP de forma estándar e interoperable

ID-WSF con servicios de identidad

- Requieren acceso a datos asociados a una identidad
  - Dicho de otro modo, el WSC accede a datos proporcionados por el WSP en nombre de un usuario concreto
- Liberty proporciona para ello el identificador de recurso (*resource identifier*)
  - Lo proporciona el Discovery Service del usuario

Descubrimiento e invocación

- Liberty define un Discovery Service junto con un protocolo para poder acceder al mismo
- Liberty ID-WSF no requiere explícitamente el uso del servicio de descubrimiento
  - Podría usarse un registro UDDI, por ejemplo
- El Discovery Service permite descubrir servicios que pertenecen a un usuario concreto
  - Utiliza el identificador del recurso para ello
- La respuesta contiene un punto de acceso al servicio, la credencial que éste requerirá e indicaciones sobre las políticas exigidas por aquel

Interacción del WSP con el usuario

- Generalmente el WSP no tiene contacto directo con el usuario
  - Pero puede necesitarlo para obtener consentimiento explícito, obtener más datos, etc.
- Liberty proporciona un Interaction Service para ello

Servicios Federados: El futuro pasa por SOA

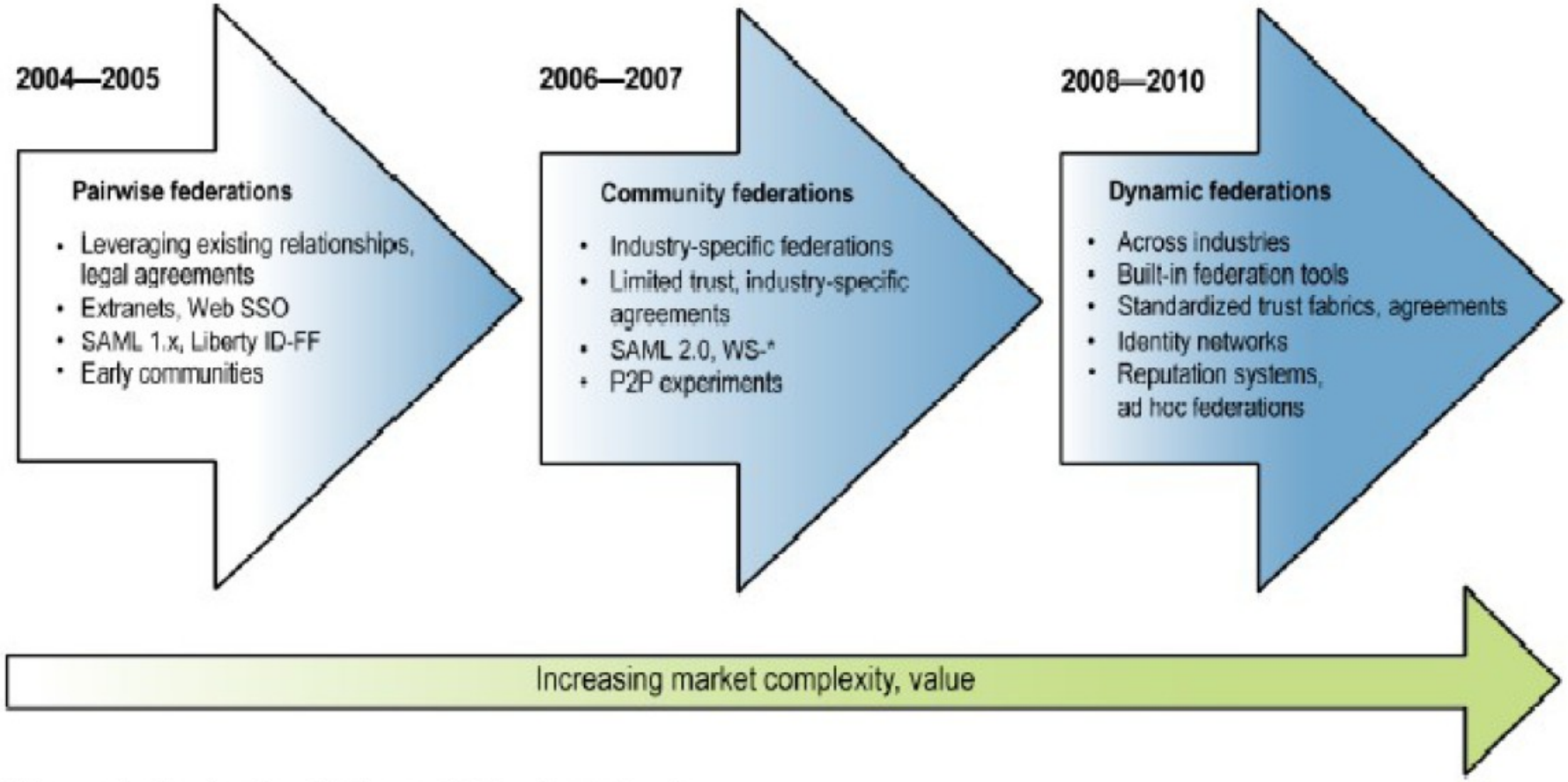
Proyecto Concordia: llevar la interoperabilidad a la capa de Identidad de Internet.

Soporte OpenSource a participantes de confianza

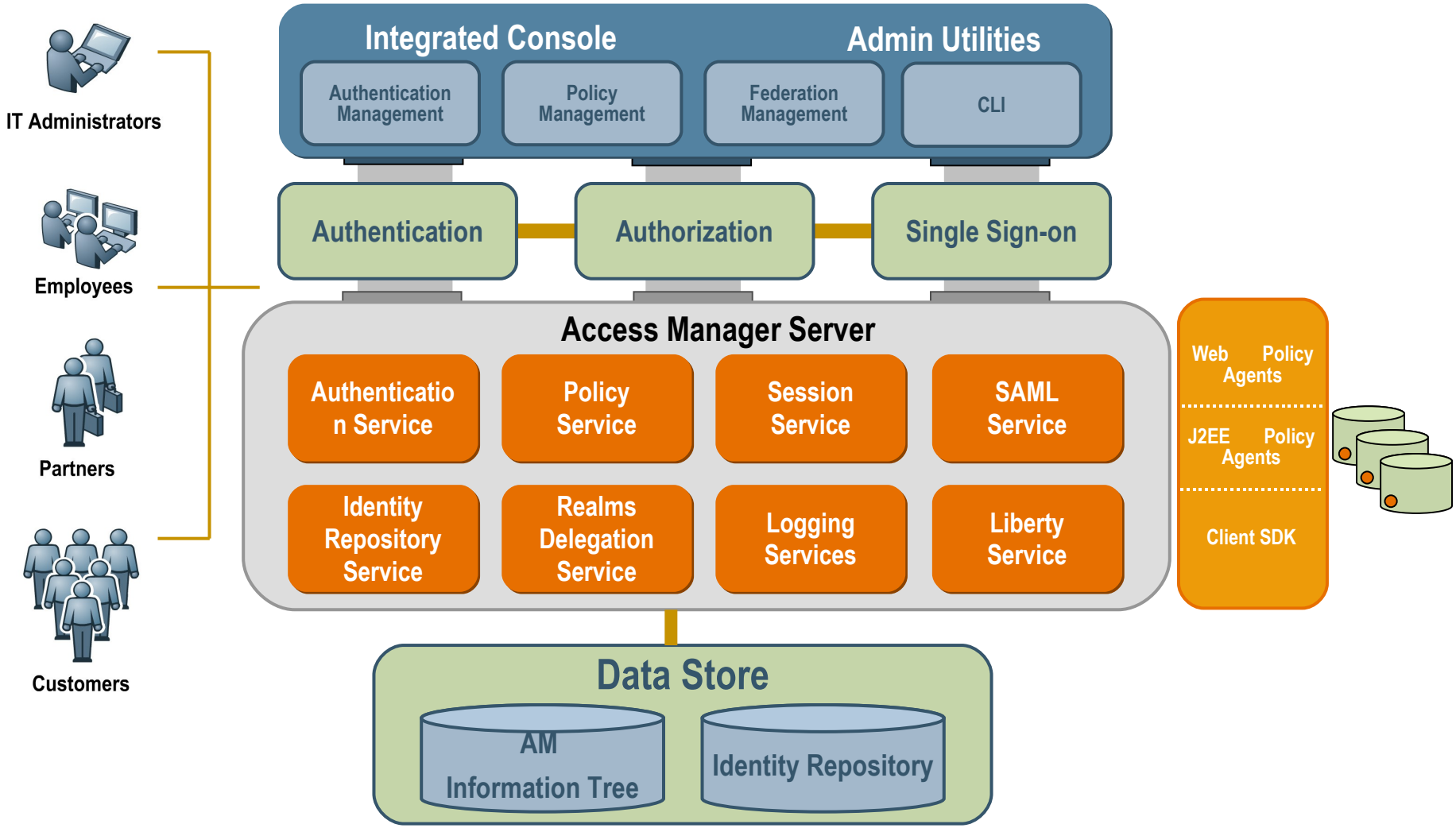
Identity Governance Framework: Regular de manera efectiva quién tiene datos personales de los usuarios, y qué permisos han dado los usuarios para el acceso a dichos datos, respetando el marco regulatorio y facilitando los procesos de auditoría.

Aproximación "User Centric" en lugar de "Internet Centric": El usuario es quien tiene el control sobre sus datos, y estos datos se utilizan para ofrecerle los servicios más adecuados en cada momento.

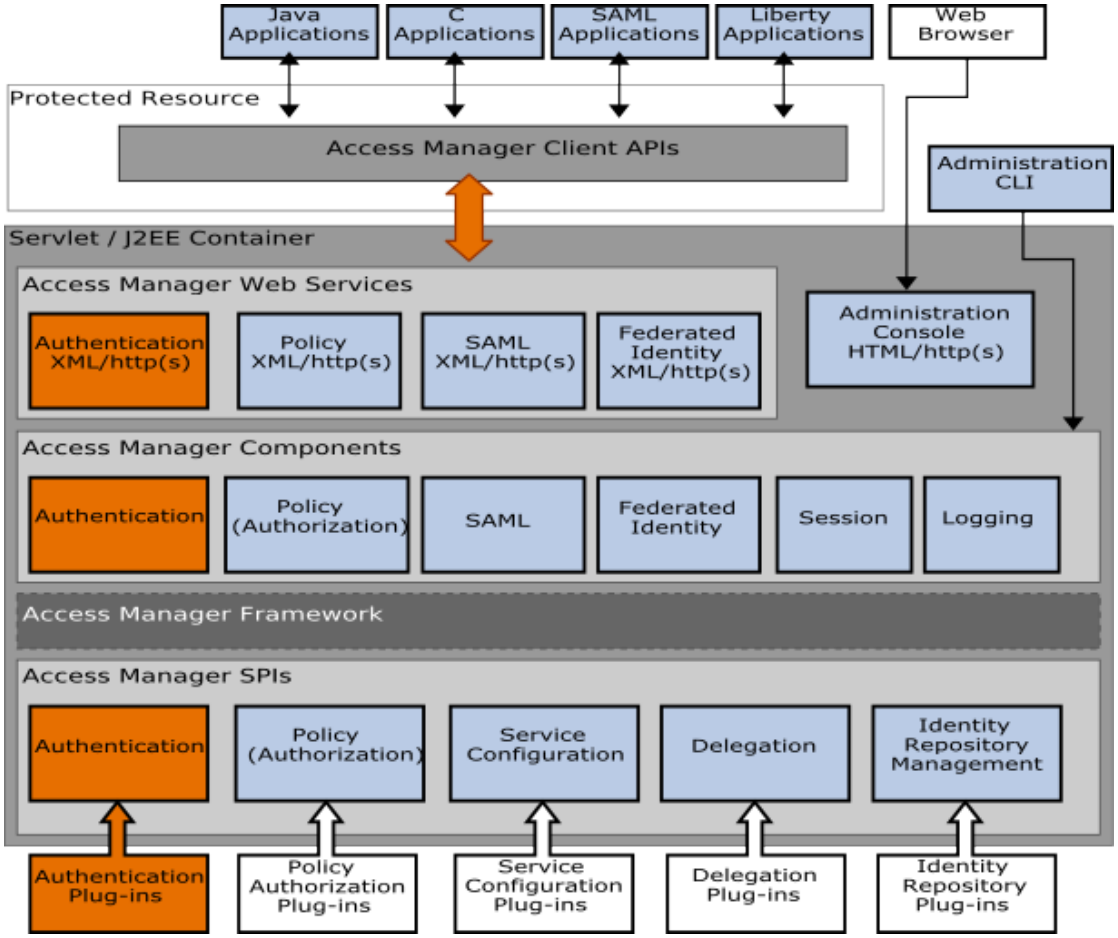
Previsión de Adopción



OpenSSO/OpenFederation: Arquitectura



Añadiendo Nuevos Servicios de Autenticación (p.ej. PAPI)



Estrategia OpenSource de Sun

http://java.sun.com/javaee

OpenPortal
Open Source. Open Standards. Open Portal Server.

Open ESB
The *Open* Enterprise Service Bus

NetBeans + Creator
Java EE, UML, JavaServer Faces, AJAX, BPEL/BPMN, PortletBuilder, Profiling, Mobility and collaboration tools to create simple or complex services

Portal Server
OpenJAVA Portal Server: Aggregation, security, mobility, collaboration, personalization, search, and device-independence

Application Server
GlassFish:Java EE 5.0, lightweight JAX-WS 2.0 JAXB 2.0, EJB 3.0, performance

Business Integration
OpenESB: JBI, BPEL, Data Transform

Message Broker:
OpenJAVA MQ

Access Manager
OpenSSO: User authentication and access control

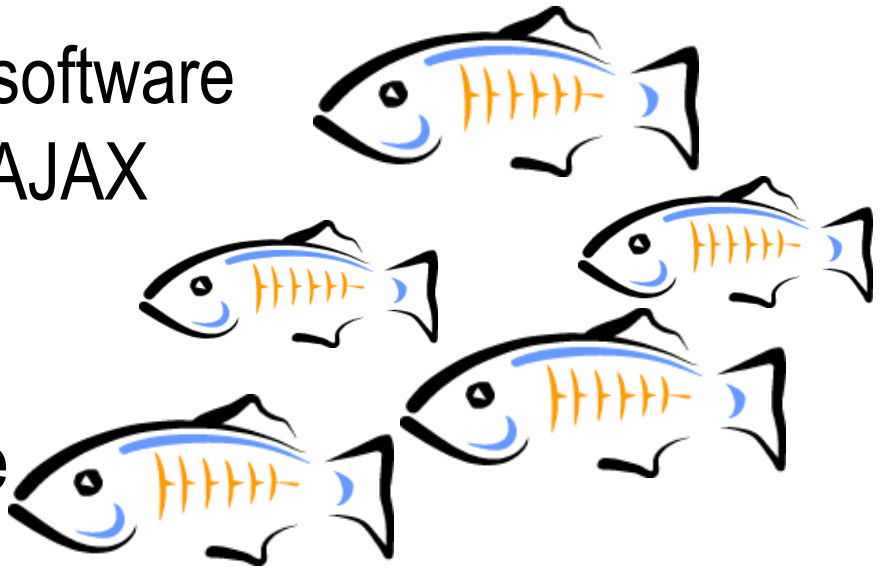
Service Registry
Store services meta data for discovery and composition

NetBeans

OpenSSO
Open Access . Open Federation

Sun FLOSS Middleware

- GlassFish – AppServer, JavaPersistence, Web Tier
- OpenPortal – Container, WSRP, Portlet, Portlet Rep
- OpenESB, OpenJBI – JBI, BPEL
- OpenSSO – Access & Fed Mgr
- OpenDS – Directory Server
- Hudson – Continuous build software
- Phobos, jMaki... – Web 2.0/AJAX
- Derby – JavaDB
- Open MQ – MessageQueue
- WoodStock – JSF Compone
- OpenInstaller



OpenSSO Status opensso.dev.java.net

- Access Manager, Single Sign-On, Federation
  - SAML, XACML, Liberty Standards
- Already Released
  - Access Manager
  - Many Policy Agents
  - Federation Manager
- To be Released
  - More Policy Agents
- *Distributed in*
  - Sun Java System Access Manager & Federation Manager

Sun OpenSource Technologies Tour

- Jornada de 2 sesiones técnicas sobre OpenSolaris y OpenSPARC en cada Centro Universitario
- Público: Directores, catedráticos y profesores de las áreas y Deptos de Arquitectura de Computadores y de Lenguajes y Sistemas, que impartan docencia en las titulaciones de Informática y de Telecomunicaciones
- Las sesiones estarían abiertas a la participación de otros profesores y alumnos (a criterio de los anteriores)

solaris™

opensolaris™

OpenSPARC™

- 50 Centros Universitarios (Facultades, Escuelas Politécnicas y Escuelas Superiores de Ingeniería), empezando por aquellos con los que ya existe un convenio de colaboración

Compromisos

- Compromisos por parte de la Universidad:
  - Inclusión en el temario de asignaturas de Arquitectura de Computadores de la tecnología OpenSPARC
  - Dirección de al menos 1 Trabajo Fin de Carrera en tecnología OpenSPARC o 1 publicación de impacto relativa a la misma
- Compromisos por parte de Sun:
  - Donación de servidor T1000 a las 15 primeras universidades que asuman el reto anterior
  - Promociones para certificar alumnos universitarios

¡GRACIAS!

Federación de Identidades: Aproximación al Entorno Educativo

isaac.moreno@sun.com