



**sabadell
universitat**

INFORMACIÓ
REFLEXIÓ
DEBAT
CONEIXEMENT

TERCERA EDICIÓ DE SABADELL UNIVERSITAT
DEL 5 AL 9 DE JULIOL DE 2004

**Registre, identificació i personalització de
serveis**

S3. Cityweb, portals de ciutat a Internet

Albert Puiggené, SBD Technologies

Sabadell, 8 de juliol de 2004

organitzadors:



patrocinadors:



Gestión e integración de la identidad de usuario

SBD Technologies

*Introducción.
Nuevas tecnologías*



www.sbdglobal.com

- **Introducción**
- Conceptos previos
- Situación actual de ejemplo
- Directorio Corporativo LDAP
- Metadirectorio
- Nuevos objetivos en la gestión de identidades
- Mecanismos y productos utilizables
- Preguntas y comentarios

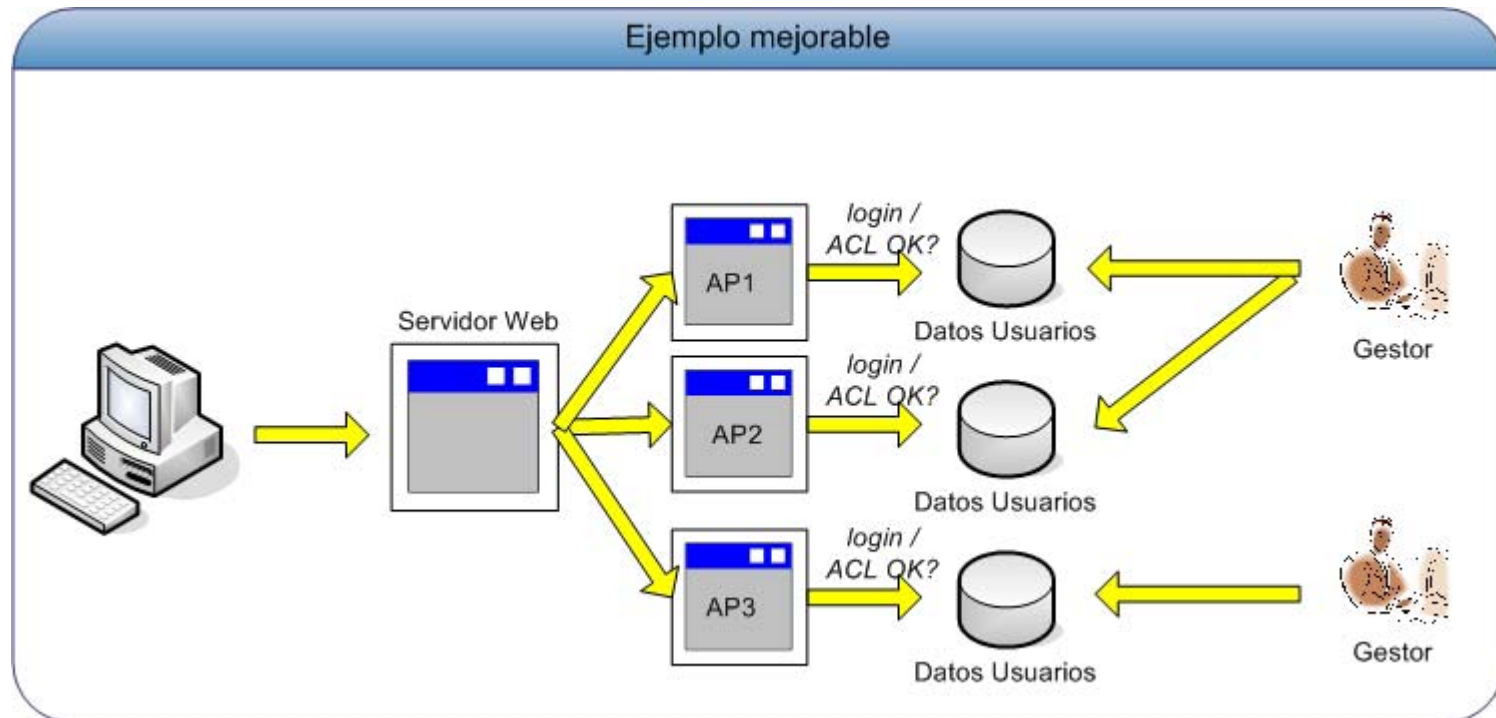
¿Qué persigue la gestión de identidades?

- Aprovisionamiento de usuarios centralizada
- Protección de la información
 - Acceso al recurso
 - ✓ Firewalls, Proxys, VLANs..
 - Autenticación del usuario
 - ✓ SmartCard con certificado, login/password, huella digital..
 - Control del acceso
 - ✓ ACLs basadas en roles, grupos..
 - Confidencialidad (secreto) de la información
 - ✓ Cifrado por SSL, 3DES, ..
 - Integridad de los datos
 - ✓ MD5, etc.
- Disponibilidad de los recursos (24x7)

- Introducción
- **Conceptos previos**
- Situación actual de ejemplo
- Directorio Corporativo LDAP
- Metadirectorio
- Nuevos objetivos en la gestión de identidades
- Mecanismos y productos utilizables
- Preguntas y comentarios

<p>Directorio único</p>	<p>Ej: RACF, Active Directory, Sun One, etc.</p>	<ul style="list-style-type: none"> -Gestión centralizada -Todos los aplicativos deben adaptarse al directorio único
<p>Varios directorios</p>	<p>-Situación usual</p>	<ul style="list-style-type: none"> -Flexibilidad para aplicativos -Coste alto de gestión (diferentes puntos de admin.) -Errores de integración
<p>Metadirectorio</p>	<p>-Uso Join Engine para replicar datos en un repositorio central desde varias fuentes</p>	<ul style="list-style-type: none"> -Flexibilidad aplicativa -Coste alto de gestión (diferentes puntos de admin.) -Reglas complejas, performance
<p>Metadirectorio virtual</p>	<p>-Metadirectorio distribuido. Ej: Calendra</p>	<p>-Ídem Metadirectorio</p>
<p>Identity management</p>	<p>-User provisioning avanzado, con tecnología estándar (http, etc.).</p>	<ul style="list-style-type: none"> -Integración con productos y soluciones. -Autenticación y autorización centralizada. -GUIs web -Gestión delegada de usuario, self-service

- Introducción
- Conceptos previos
- **Situación actual de ejemplo**
 - Directorio Corporativo LDAP
 - Metadirectorio
 - Nuevos objetivos en la gestión de identidades
 - Mecanismos y productos utilizables
 - Preguntas y comentarios



- Introducción
- Conceptos previos
- Situación actual de ejemplo
- **Directorio Corporativo LDAP**
- Metadirectorio
- Nuevos objetivos en la gestión de identidades
- Mecanismos y productos utilizables
- Preguntas y comentarios

- **LDAP**: Lightweight Directory Access Protocol
- Protocolo utilizado para acceder a servicios de directorio, específicamente X.500 (servicio de directorio OSI)
- **TCP/IP**
- Basado en entradas, cada entrada es un conjunto de atributos (dn, cn, mail, etc.)
- Estructuración jerárquica de la información

- Versatilidad para **almacenar entidades de muy diversa naturaleza** y la facilidad con la que puede ampliarse la información de cada entidad según sea necesario
- **Facilidad de sincronización con otros repositorios**, ya sean otros directorios LDAP, bases de datos relacionales, etc.
- Varias **funcionalidades** referentes a la política de **seguridad**:
 - Usuarios, contraseñas, diferentes posibilidades de políticas sobre contraseñas (caducidad, número caracteres mínimo, etc.)
 - ACLs y ACIs
 - Perfilado de usuarios, asignación a roles
 - Administración distribuida y delegada (en función de estructura)
- **Elevada eficiencia** en la realización de **consultas** puntuales

Microsoft Active Directory 2002

- Componente de SO Windows
- Servicio de directorio que soporta LDAP y Kerberos para la autenticación de usuarios
- Integración con el logon en Windows
- Punto centralizado para la gestión de cuentas, clientes, servidores y aplicaciones
- Proporciona posibilidades de SSO a los usuarios (autenticación, PKI, smart cards, etc...)
- Basado en SQLServer
- No tiene sentido sin dominio Windows

Sun One Directory Server 5.2

- Soporta los principales estándares de comunicación (LDAP v3, DSMLv2, etc...)
- Soporte para varias plataformas
- Integración Windows
- Alto rendimiento en búsquedas, con diferentes tipologías de índices (presencia, igualdad, substring, etc...)
- Multitud de posibilidades para la definición de ACLs, ACIs, búsquedas dinámicas, etc.
- Características avanzadas de seguridad (multipassword, reseteo password, encriptación, etc...)
- Soporte PKI, kerberos
- Replicación master/slave, multi-master, alto rendimiento

IBM SecureWay Directory Server

- Soporta los principales estándares de comunicación (LDAP v3, DSMLv2, etc...)
- Soporte para varias plataformas (incluidas host IBM)
- GUI web
- Alta integración IBM OS, middleware WebSphere y Tivoli
- Soporta autenticación basada en credenciales, certificados digitales y Kerberos
- Control de acceso a nivel de atributo (ACLs), administración delegada
- Funcionalidades básicas sobre gestión de password
- Replicación robusta entre master/slave, cascada y p2p. Multimaster

Otros: Critical Path, Novell eDirectory, Open LDAP

- Introducción
- Conceptos previos
- Situación actual de ejemplo
- Directorio Corporativo LDAP
- **Metadirectorio**
- Nuevos objetivos en la gestión de identidades
- Mecanismos y productos utilizables
- Preguntas y comentarios

Problema

- ▶ La **información de empleados** y otros datos de su organización se encuentra **descentralizada** entre las diversas **bases de datos orientadas a servicio**
- ▶ **Mantenimiento complejo** y la información no está siempre sincronizada entre los diversos servicios.
- ▶ **No** es viable **prescindir** de estas bases de datos orientadas al servicio

Solución

- ▶ Definir un repositorio que sea capaz de **concentrar la información** de todos estos servicios y **propagar los cambios** de información compartida entre las diversas bases de datos orientadas a servicio
- ▶ Este repositorio central de información de directorio suele ser un directorio **LDAP** en el que cada entidad puede contener información de varios servicios
- ▶ Las **fuentes de información** de este repositorio son **muy diversas** (LDAP, bbdd, ficheros, Notes, Host, etc...)

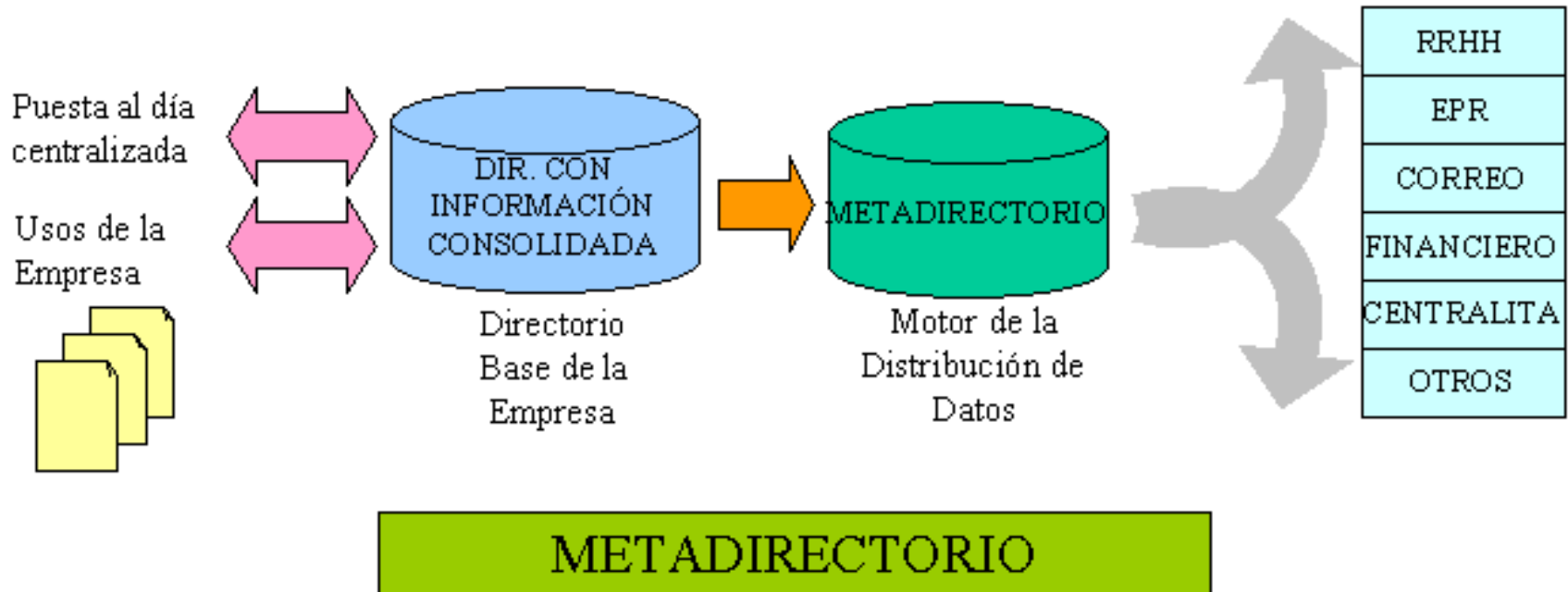
- Un Metadirectorio **es un servicio de directorio** que puede integrar a su vez múltiples servicios de directorio en una organización
- **Directorio de directorios**, que actúa como la fuente autoritativa y centralizada de información
- Los distintos repositorios le **notifican** los cambios producidos y es capaz de **propagarlos** a donde sea necesario
- La base de un metadirectorio puede ser:
 - Un directorio cualquiera promocionado
 - Una solución de metadirectorio propietaria
- A un Metadirectorio se le establecen **reglas** que permiten **relacionar las entradas del repositorio central con las diferentes fuentes de información**. También se le especifican reglas sobre los atributos compartidos y sobre la periodicidad y dirección en la que se realizan los cambios.

- **Centralización de la información corporativa** (usuarios, perfiles, recursos, etc.)
- **Administración centralizada** y posibilidad de delegación
- **Sincronización y replicación de la información** entre distintos repositorios de información (directorios LDAP, bases de datos, otras aplicaciones, etc.). Las modificaciones realizadas por las aplicaciones únicamente deben realizarse en un solo repositorio
- Se **evita duplicidad** de información y errores asociados a su gestión
- **Agregación en un único repositorio** de información de perfilado referente al usuario, a partir de varios repositorios
- Existe **un único directorio** con toda la información corporativa consolidada

- La **implementación** de una solución de **Metadirectorio** debe realizarse por **etapas**.



- Los repositorios origen de información deben proporcionar mecanismos estándares para la **detección en tiempo real de los eventos de actualización** producidos sobre las distintas entidades
 - Triggers Oracle, Change log LDAP (rama LDAP consultable con los cambios producidos en el directorio), etc.
- De la misma forma, los repositorios destino deben proporcionar mecanismos estándares para la **actualización externa de información**.
 - DSML, XML, SQLNet, etc.
- El **repositorio de consolidación** (sobre el que se basa el metadirectorio) debería ser **LDAP**



Critical Path Metadirectory server

- Independiente del repositorio de consolidación
- Poco intrusivo
- Seguridad basada en SSL (si es soportado por la fuente)
- Alto grado interoperatividad: varios conectores para diferentes productos comerciales (LDAP, BD, RACF, etc.)
- Posibilidad de desarrollar conectores
- Uso de una avanzada GUI para el diseño de reglas de negocio.
- La fuente autoritativa se define por cada atributo

Novell DirXML (eDirectory)

- El repositorio de consolidación debe ser eDirectory
- Poco intrusivo
- Seguridad basada en SSL o mediante plugin instalado
- Alto grado interoperatividad
- Posibilidad de desarrollar conectores
- GUI poco útil, debe programarse las reglas de negocio
- La fuente autoritativa se define por cada atributo

Microsoft Metadirectory server

- Utiliza Active Directory como repositorio de consolidación
- Idóneo para sincronización entre diferentes Active Directory, aunque no recomendado para otros repositorios
- Grado de interoperatividad relativo (pocos conectores)
- GUI útiles para definir reglas de negocio

Otros: Sun One Metadirectory Server

Causas

- ▶ El ritmo de **crecimiento** de las **tecnologías** en una entidad es **elevado** y no se realiza un plan estratégico de asimilación de las mismas
- ▶ **Diferentes aplicaciones** / sistemas requeridos por negocio son implantadas. Cada aplicación dispone de un **repositorio propio** de **usuarios**
- ▶ **No** se establece una **política** e infraestructura de **gestión** de **usuarios** eficiente y centralizada

Problema

- ▶ Los **usuarios** deben gestionar **multitud** de **identificadores** de usuarios y contraseñas
- ▶ Los usuarios eligen **contraseñas sencillas** para memorizar, poniendo potencialmente en peligro la seguridad del sistema
- ▶ **Administración descentralizada**

Solución

- ▶ Identificador de usuario y contraseña **única**.
- ▶ **Centralización** de **repositorios**, facilitando la gestión de usuarios.
- ▶ Adaptación de las aplicaciones/sistemas para utilizar el **repositorio centralizado** de usuarios
- ▶ **Sincronización** de contraseñas para aquellos sistemas que no puedan ser adaptados

- **Single Sign On**

- El usuario posee una única contraseña y realiza una única autenticación para el acceso a todos sistemas.

Se requiere simulación de sesión por un componente centralizado donde se realiza la autenticación o confianza por parte de los sistemas

- **Simple Sign On**

- El usuario tiene una única contraseña, pero debe realizar una autenticación para cada sistema (introduciendo la misma contraseña).

Se requieren mecanismos de réplica de contraseñas, adaptación de los sistemas de cambio y restauración de contraseña, etc...

- **Sincronización contraseñas entre repositorios**
 - Mediante el uso de **productos comerciales o desarrollos a medida**. Se debe estudiar la viabilidad en cada caso
 - Debe tenerse muy en cuenta la **afectación a la seguridad del sistema** (protocolos para la sincronización, etc.)
 - La **sincronización debe ser on-line**
 - Debe existir **homogeneidad en las restricciones de contraseñas** (núm. caracteres, etc.)
- **Automatización inicio sesión**
 - La autenticación en el sistema comporta **establecer o simular una sesión** para cada una de las aplicaciones a integrar en el SSO, de forma **transparente** al usuario
 - Necesidad de constar con un **sistema centralizado de usuarios** donde se definan privilegios y sistemas a los que puede acceder, además de un componente encargado de establecer o simular sesiones.
- **Autenticación por tokens (Kerberos)**
 - Sistema de autenticación mediante tokens. Permite a usuarios y servidores identificarse los unos a los otros a través de un intermediario que goza de total confianza, denominado KDC (**Kerberos Key Distribution Center**)
 - El KDC de Kerberos emite tokens que permiten autenticar a los clientes y a las claves temporales de sesión que éstos utilizan como claves temporales de codificación durante las sesiones de inicio. El token de un usuario es único y no funciona con los restantes usuarios.

Requisito

Restringir la visibilidad de determinados documentos, aplicaciones o sistemas a los usuarios en función de perfiles o roles

- de **forma unificada** (la misma para cada aplicación)
- con **una administración** (asignación de perfiles/roles a usuarios y recursos) centralizada en mismo sistema pero distribuida y delegada a diferentes administradores

Situación usual

Cada aplicativo **gestiona su propia política de control de acceso** sobre los recursos protegidos

- Tediosa administración y procesos complejos
- Replicación de información (usuarios, perfiles, etc...) y incongruencia de la misma

Solución

Proporcionar un mecanismo que intercepte las peticiones y determine si el usuario tiene autorización para acceder al recurso solicitado:

- Requiere un sistema centralizado de autenticación, que mantenga la sesión de los usuarios
- Requiere un repositorio único de usuarios, recursos y perfiles (LDAP)

