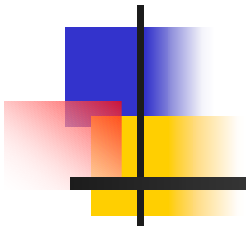
GT RedIRIS 2003
"Middleware"

4/11/2003



Sistema Autenticación Centralizado basado en LDAP de la UNED. Integración de aplicaciones

José Carlos Remiro

Centro Servicios Informáticos - UNED

jcremiro@csi.uned.es

La UNED en cifras (I)

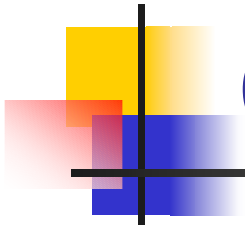
- Alumnos
  - 155.000 alumnos enseñanzas regladas
  - 2.500 en el extranjero
  - 30.000 alumnos de educación permanente
- Personal
  - 1.200 PAS sede central
  - 1.300 PDI sede central
  - 5.700 profesores tutores de centros asociados

La UNED en cifras (II)

- Cursos
  - 22 titulaciones oficiales
  - 1823 asignaturas
  - 106 programas de doctorado
  - 484 cursos de educación permanente
- Centros
  - 3 campus en Madrid
  - 60 centros asociados en españa
  - 20 centros asociados en el extranjero

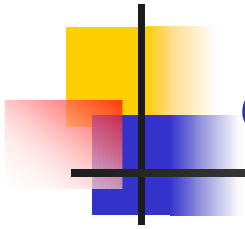
¿Por qué cambiar a un sistema de autenticación único?

- Puesta en marcha de nuevas aplicaciones con cientos de miles de usuarios.
- Simplicidad de gestión para identificadores /passwords.
- Mejora de la seguridad.
- Centralización del proceso de autenticación.
- Presentación de aplicaciones cómo parte de un único servicio



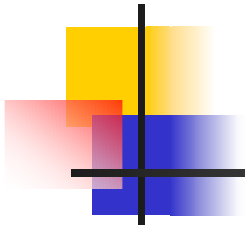
Gestión de identificadores

- Alumnos de Enseñanzas Regladas
  - Secretaría virtual
  - Identificadores significativos
- Personal de la UNED
  - Correo electrónico
  - Identificadores usuario máquina correo
- Resto de usuarios
  - Aún sin tratar



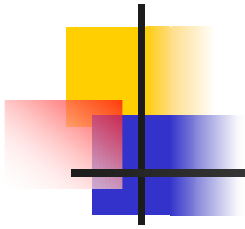
¿Por qué utilizar LDAP?

- Se encuentra optimizado para la operación de lectura
- Extensible
- Permite la réplica
- Rendimiento
- Estándar



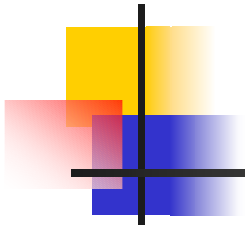
LDAP de la UNED: estructura

- Software: OpenLdap 2.0.27
- Estructura:
  - Raíz:
    - dc=uned, dc=es
  - Ramas:
    - ou=Administradores (7 entradas)
    - ou=Personas (220.000 entradas aprox.)
    - ou=Internos (8000 entradas aprox.)



LDAP de la UNED: esquemas

- inetorgperson.schema
- nis.schema
- rfc822-MailMember.schema
- autofs.schema
- kerberosobject.schema
- courier.schema



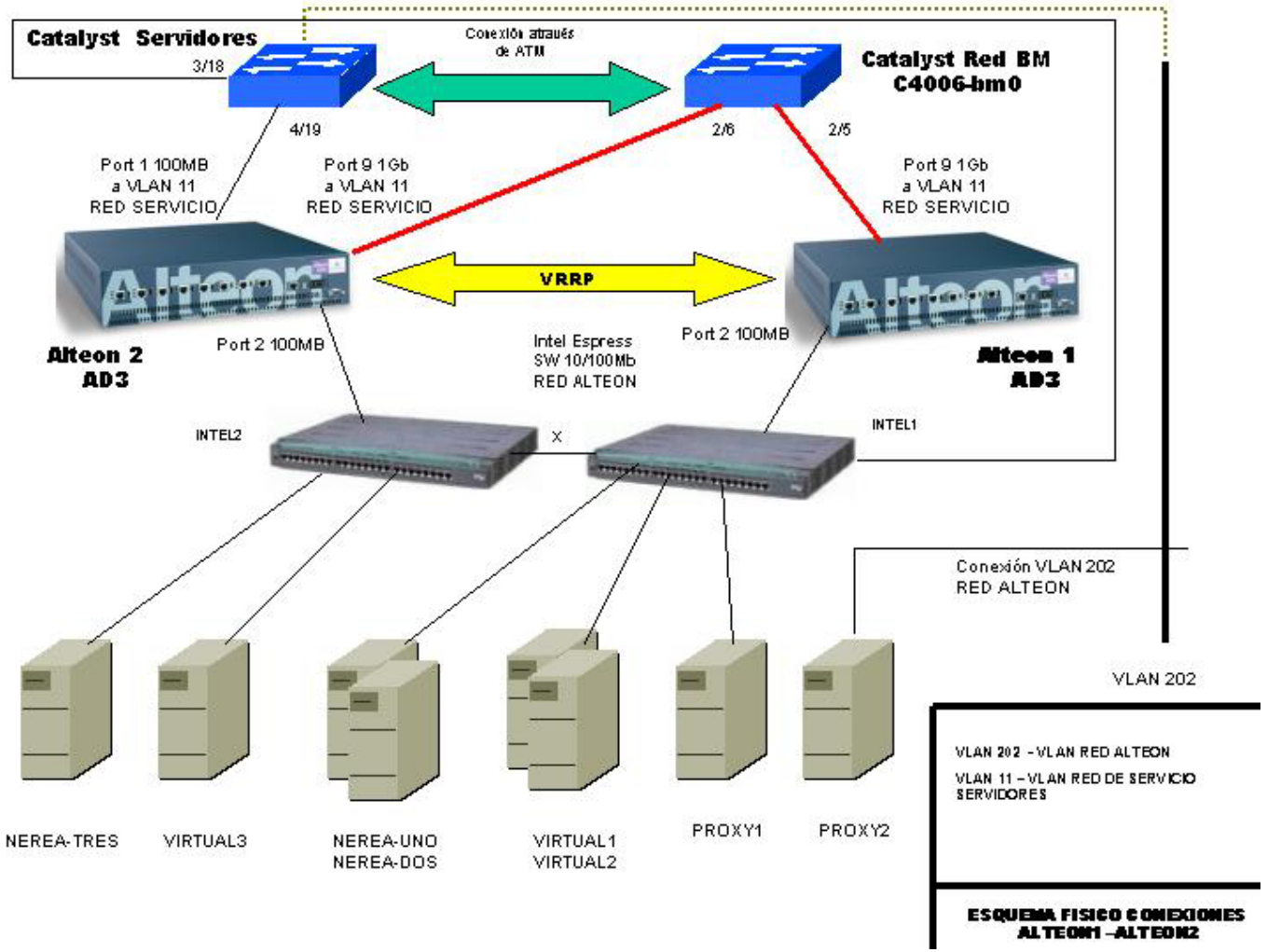
LDAP de la UNED: permisos

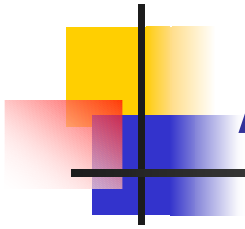
- Todos los usuarios puedan “bindarse” con el atributo userPassword.
- Todos los usuarios una vez autenticados pueden leer todos sus atributos.
- El atributo userPassword únicamente puede ser leído por usuarios privilegiados.
- Los administradores con privilegios pueden modificar las entradas y escribir en el directorio.

LDAP de la UNED: opciones de optimización

- Tamaño para la caché de 100 MB
- Tiempo de inactividad máximo por conexión 60 minutos
- Número total de threads 189
- Creación de índices para los atributos uid, mail y objectClass

LDAP de la UNED: esquema físico

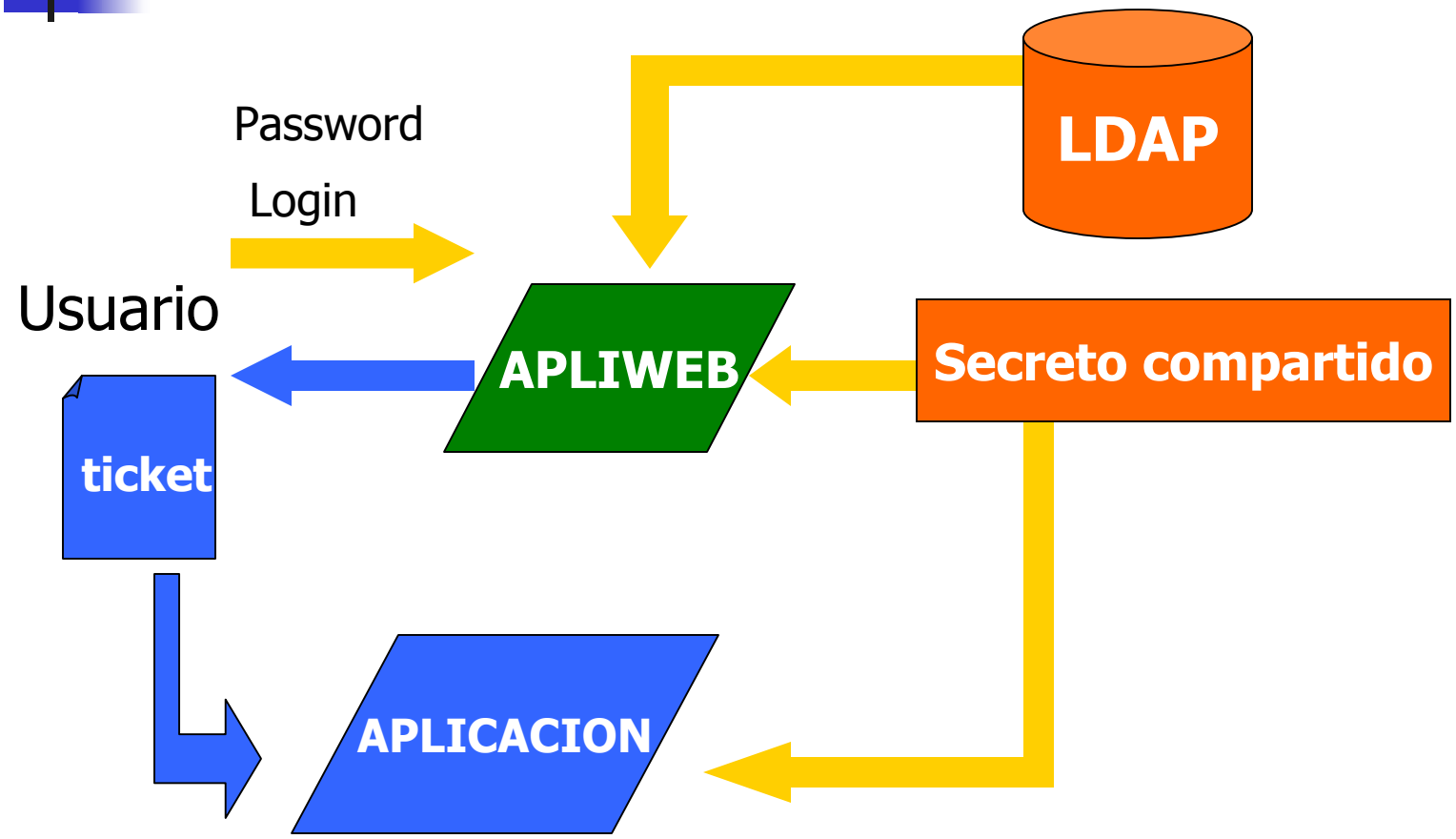




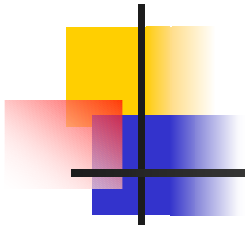
Autenticación y autorización

- Actualmente, existen dos aplicaciones encargadas de autenticar usuarios:
  - Apliweb.- Punto de acceso de los alumnos
  - CiberUned.- Punto de acceso del personal de la UNED
- Todas las aplicaciones son responsables del proceso de autorización.
- Salvo el servicio de correo, todas las aplicaciones son responsables de gestionar los parámetros de configuración del usuario

Esquema del proceso de autenticación

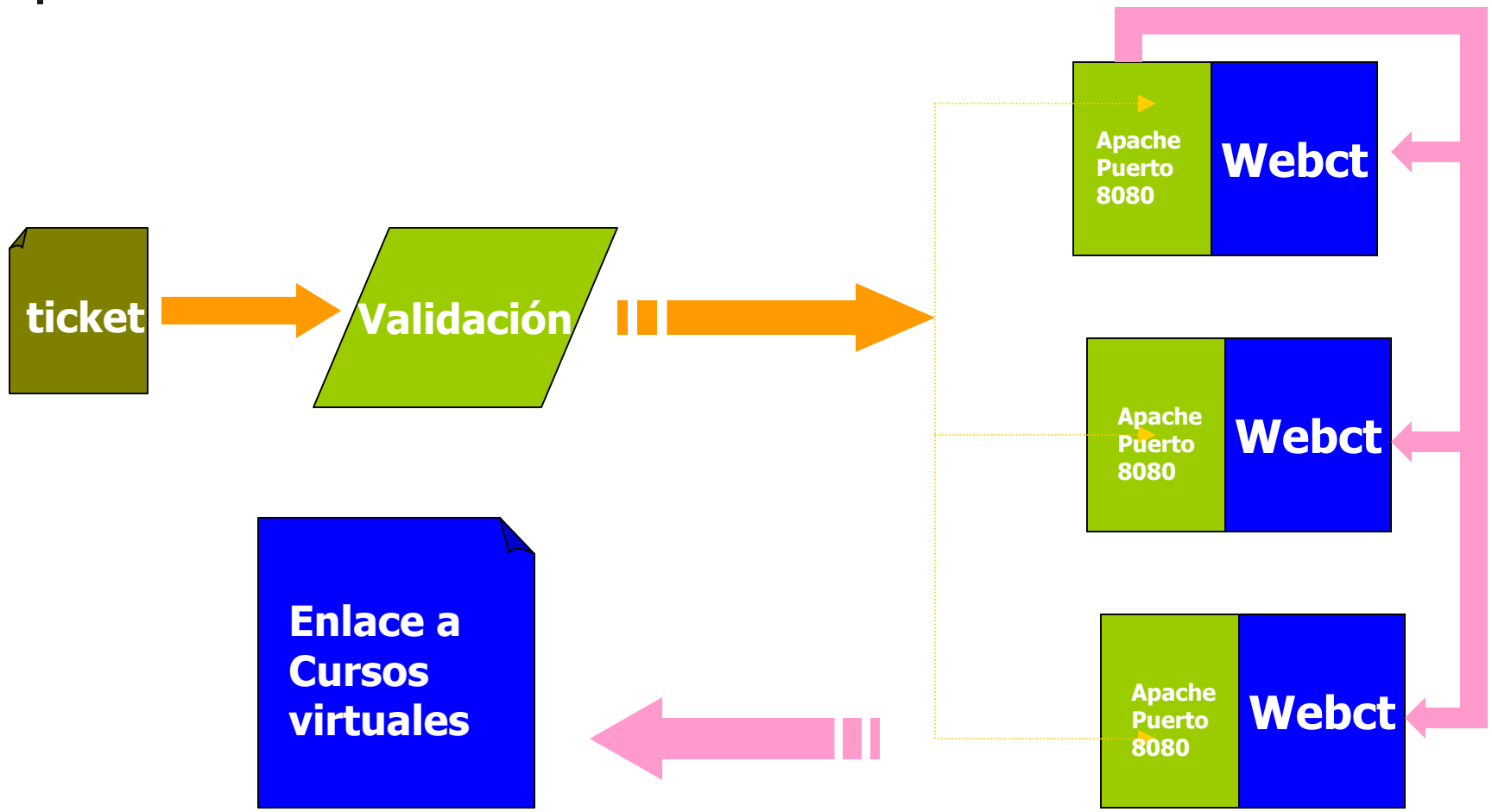


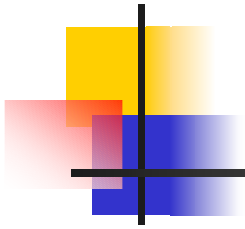
El ticket generado por el proceso de autenticación



- Se encuentra formado por una cadena de caracteres, cuyos campos se encuentran separados por el símbolo '#'.
- Entre los campos del ticket se encuentra el identificador de usuario, el timestamp y un valor que permite validar el ticket.
- La debilidad del sistema se encuentra en el secreto compartido.

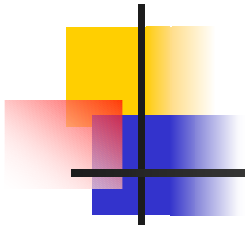
Ejemplo de autorización: Cursos virtuales de la UNED





Problemas del sistema actual

- Se dan casos aislados de usuarios que disponen de más de un identificador.
- Falta integrar usuarios en el sistema.
- El secreto compartido puede convertirse en un “secreto a voces”.
- Faltan aplicaciones por integrar en el sistema
- Existen aplicaciones que podrían beneficiarse del sistema si se ampliasen los esquemas.



En fase de estudio

- Inclusión de nuevos esquemas en los servidores LDAP.
- Modificación del contenido del ticket para utilizar clave publica/privada.
- Adaptación de aplicaciones para su integración en el esquema de autenticación centralizado.
- Solución del problema de usuarios con identificadores múltiples.