



VOs en IRISGrid

Modelo arquitectónico de certificación



RedIRIS

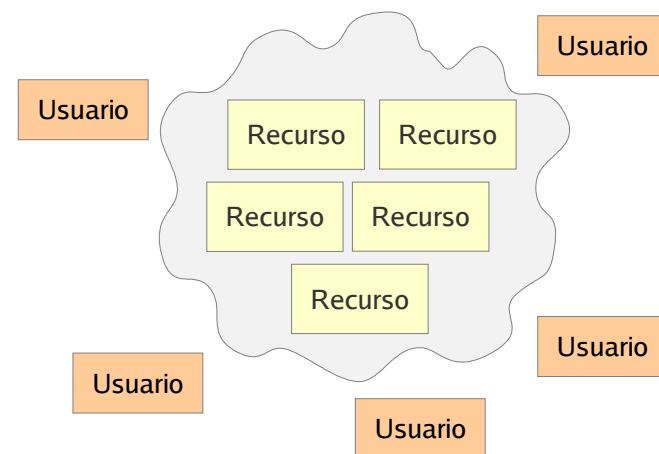


- IRISGrid

- Proporcionar a los usuarios mecanismos para un acceso simple, ubicuo e integrado a todos los recursos disponibles

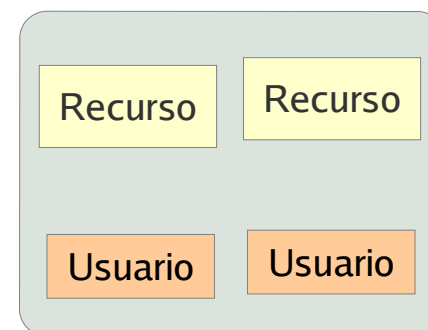
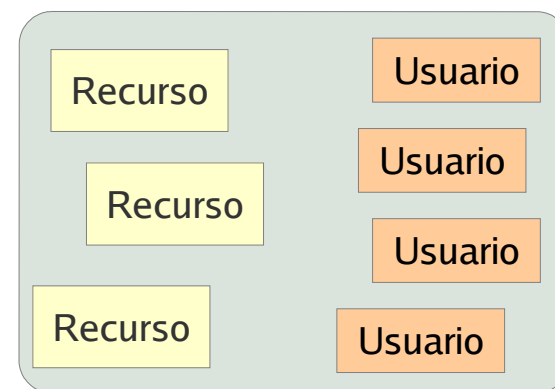
- ¿A qué hemos llamado recursos en IRISGrid?

- Acceso a la red
- Recursos de computación
 - Cálculo distribuido, supercomputadores, librerías específicas, ...
- Recursos de almacenamiento
 - Temporal o permanente
- Recursos de información
 - Bibliotecas electrónicas, buscadores y metabuscadores, ...
- Recursos de interacción
 - Servicios de video y multi-conferencia, escritorios virtuales, ...

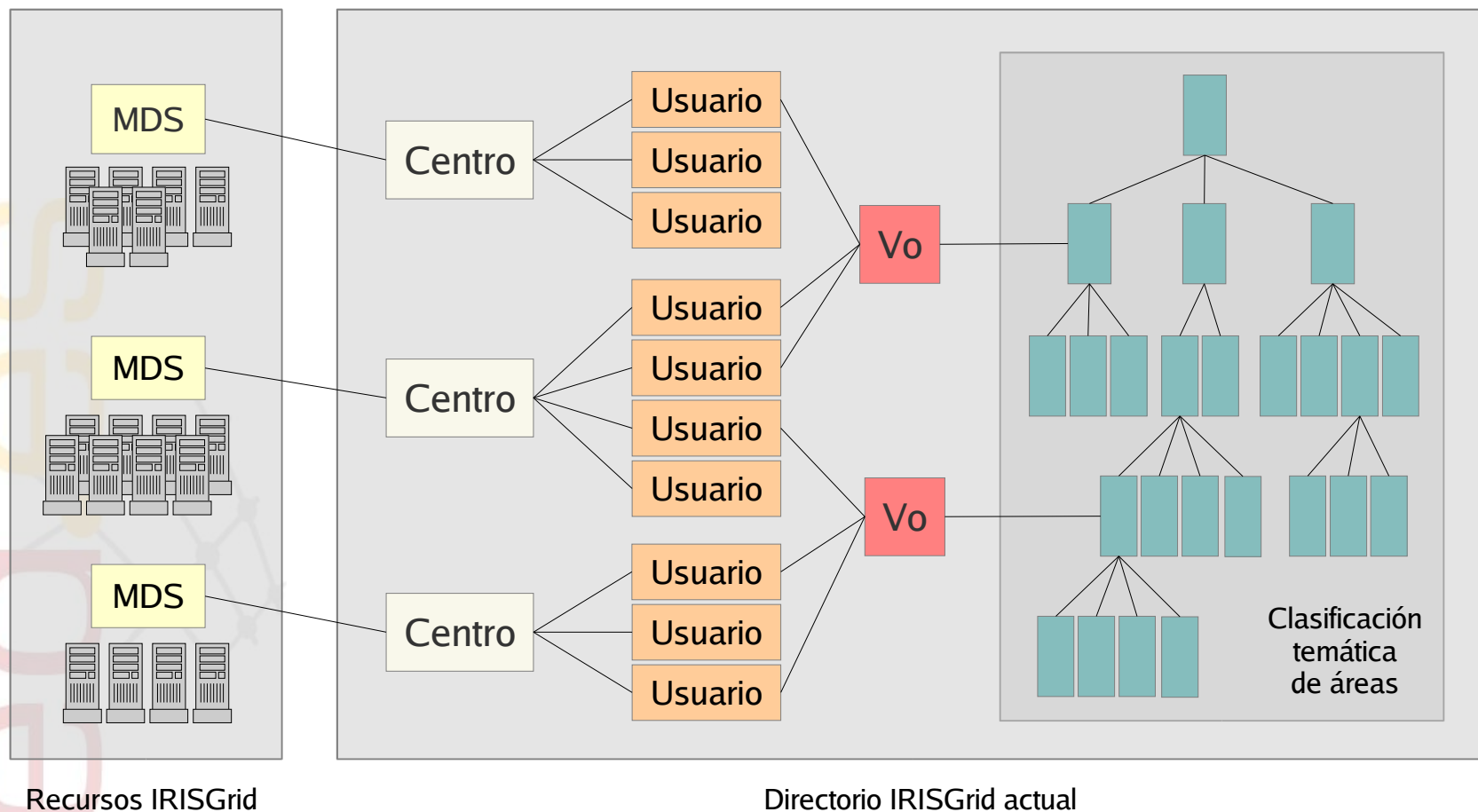


- **Objetivo**
 - Cualquier usuario pueda obtener en cualquier punto el servicio de una manera simple
- **La localización de los recursos no es lo único importante**
 - Recursos distribuidos
- **Lo más importante son los mecanismos para integrarlos**
 - Autenticación - Establecer la identidad de los usuarios y servicios
 - Autorización - Determinar los derechos de los usuarios
 - Localización - Encontrar los recursos
 - Contabilidad - Registrar el uso de los recursos
 - Optimización - Racionalizar el uso de los recursos
 - Gestión - Actuar sobre recursos y mecanismos de acceso
 - Seguridad - Garantizar la disponibilidad y buen uso

- **Un conjunto de usuarios**
 - Asociados a una misma área temática
 - Comparten similares necesidades
 - Acceso al procesado de datos
 - Acceso a datos y recursos distribuidos
 - Persiguen objetivos similares
- **Un conjunto de recursos**
 - Cálculo
 - Almacenamiento
 - Información
 - Otros
 - Operación remota de dispositivos
 - Conocimiento
 - ...

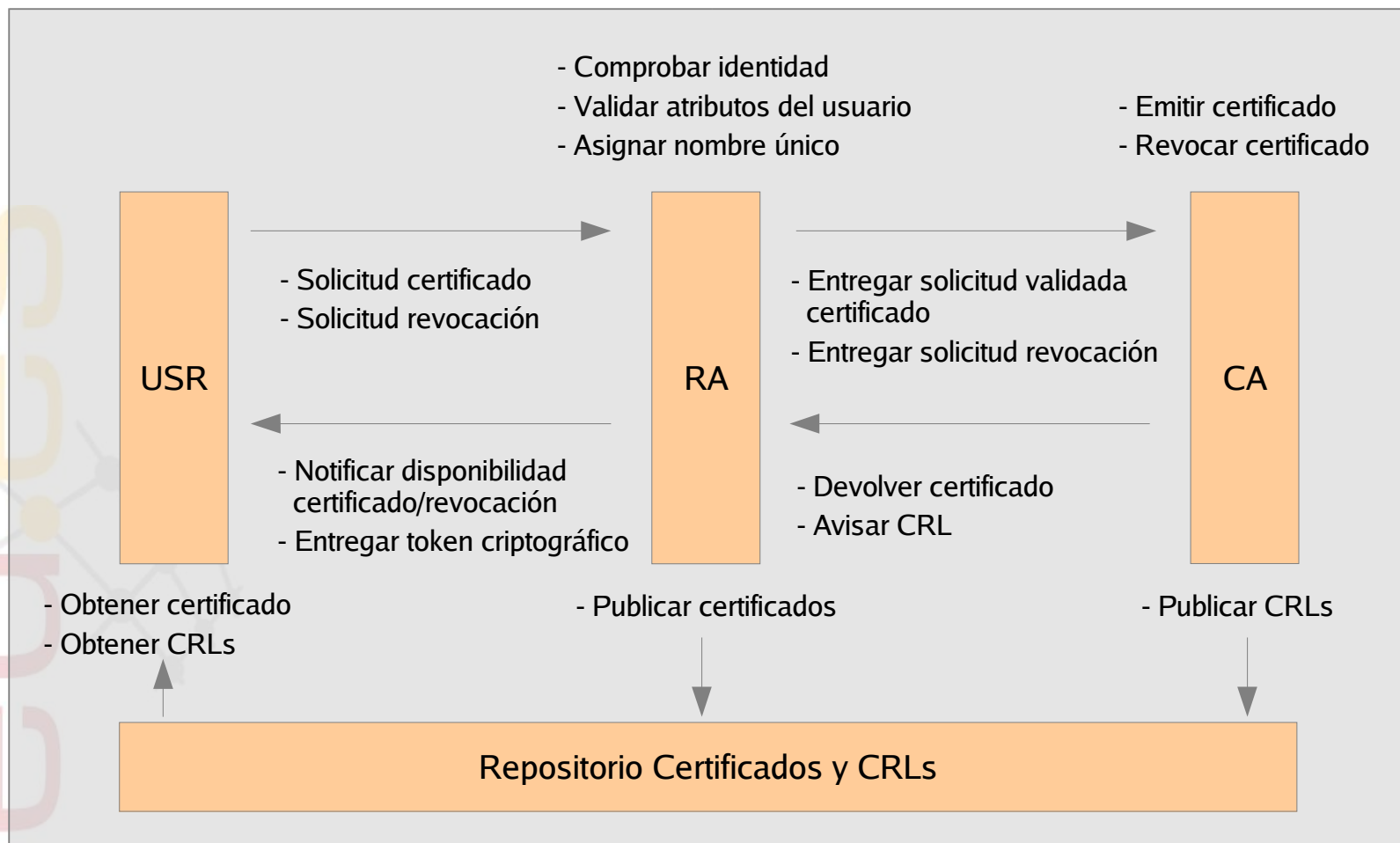


- **Son la base para una infraestructura dinámica que permita**
 - Incorporar centros donde haya usuarios y recursos
 - Administradores de Centros que den de alta a sus usuarios
 - Crear VOs y áreas temáticas
 - Relacionar las VOs con las áreas temáticas
 - Administradores de VOs que incorporen a los usuarios a las VOs
 - Dueños de recursos que los compartan en las Vos
 - Buscar, localizar e interaccionar con los usuarios
 - Buscar, localizar y acceder a los recursos
- **Esta infraestructura dinámica es el Directorio IRISGrid**
 - Como los recursos y usuarios se añaden/borran/cambian de manera dinámica la estructura debe permitirlo



- **¿Qué es EUGridPMA?**
 - European Policy Management Authority for Grid authentication in e-science
- **Objetivo**
 - Establecer unos requisitos y buenas prácticas para los proveedores de identidad grid que genere un entorno de confianza que pueda ser aplicado a la autenticación de entidades finales en un entorno inter-organizacional para el acceso a recursos distribuidos
- **Ventajas**
 - Equivalencias con todas las CAs de EUGridPMA
 - Compatibilidad automática con EGEE
 - Compatibilidad con DataGrid-ES (IFCA)
 - Compatibilidad con futuros proyectos Grid
 - Europeos y globales

- **Las CAs que estén en EUGridPMA serán equivalentes**
 - Tienen políticas que cumplen unos mínimos comunes
 - No necesitamos jerarquías complicadas de certificación
 - Nos fiamos de esas CAs pero no de las que las hayan certificado
 - Usaremos TACAR como fuente fiable de certificados y políticas
- **Requisitos mínimos**
 - Estructura PKI
 - Autoridad de Certificación
 - Espacio nombres, Políticas, Requisitos clave y certificados, CRLs, ...
 - Autoridad de Registro
 - Identidad usuario, unicidad nombres, comunicaciones seguras con la CA
 - Certificados de entidad final
 - Clave generada por el usuario, 1 año, información políticas



- **Controles de seguridad**
 - Posibilidad portatil
- **Espacio de nombres**
 - dc=irisgrid,dc=rediris,dc=es
- **Políticas/Documentación**
 - 1.3.6.1.4.1.7547.2.1.4.X - Sucesivas versiones de IRISGrid-CA
 - 1.3.6.1.4.1.7547.2.2.4.X.X - IRISGrid-CA CPS versión X.X
- **Certificados**
 - Expedirlos
 - Almacenar los certificados emitidos y las fechas de revocación de los mismos
 - Revocarlos
 - Publicar información de revocación periódicamente

- RAs alojadas en RedIRIS (web) o externas (mail, WS, ...)
- Funciones
 - Identificación de entidad
 - Cada gestor/operador de RA debe conocer a sus usuarios
 - Validar identidades finales y atributos
 - Asignación de nombres. Unicidad de nombres
 - No existe un sistema global de nombres que permita identificar a todo el mundo sin ambigüedad. ¿Qué tipo de nombre usamos? (X.500, email, url, uid ...) ¿eduPersonPrincipalName o irisPersonalUniqueID?
 - eduPersonPrincipalName= javi.masa@rediris.es
 - DN: eduPeronPrincipalName=javi.masa@rediris.es,dc=irisgrid,dc=rediris,dc=es
 - Entregar las solicitudes validadas a la CA
 - Publicar certificados
 - Notificar al solicitante la disponibilidad del certificado/revocación

- Una RA estará relacionada con un Centro (OU)
 - Debe tener una entrada de centro en el directorio
- Para estar en una VO es necesario haber sido de alta por un Centro (OU, RA)
- Cuando la CA genera el certificado
 - Se creará la entrada del usuario en el directorio IRISGrid
 - Se almacena su certificado y el DN
- El responsable de VO podrá asignar entradas, ya existentes en el directorio, a su VO
 - ¿Cómo me doy de alta en una VO?
- RedIRIS podría gestionar un servicio de OU virtual (*catch-all*)

- **Esquema LDAP irisgrid**
 - <http://www.rediris.es/ldap/esquemas/>
- **Navegadores (provisional)**
 - <http://www.rediris.es/ldap/ldap-es/irisgridnav>
 - <http://www.rediris.es/ldap/ldap-es/giisnav>
- **Mail**
 - javier.masa@rediris.es

