

Jornadas Técnicas de RedIRIS
Granada, 16 noviembre 2006

pkIRIS

*Una nueva forma de
gestionar certificados*

pkIRIS
secured by galipollo

Sebastián Balboa García
sebastian.balboa@cica.es



- ¿Que es pkIRIS?
- ¿Por que pkIRIS?
- Tecnología usada en pkIRIS
- Módulos de pkIRIS
- Flujograma de uso
- Flujograma gráfico
- Esquema LDAP pkiris.schema
- Estado del proyecto
- Futuras versiones

- pkIRIS

- Software de gestión de una infraestructura de clave pública (PKI)
- Disponible bajo la licencia GNU GPL
- Surge a primeros de 2005
- Para cubrir las necesidades del CICA (en lo que respecta a firma digital de correo electrónico y autenticación de usuarios y servidores) y de RedIRIS (en el proyecto de GRID nacional, IRISGrid)

- **Requisitos**

- Distribución
 - Lógica RAs (y física)
- Simplicidad
 - Instalación del sistema
 - Creación de RAs
 - Gestión de RAs para administradores RA
 - Comunicación RA<->CA para los administradores

- **Situación a finales de 2004**

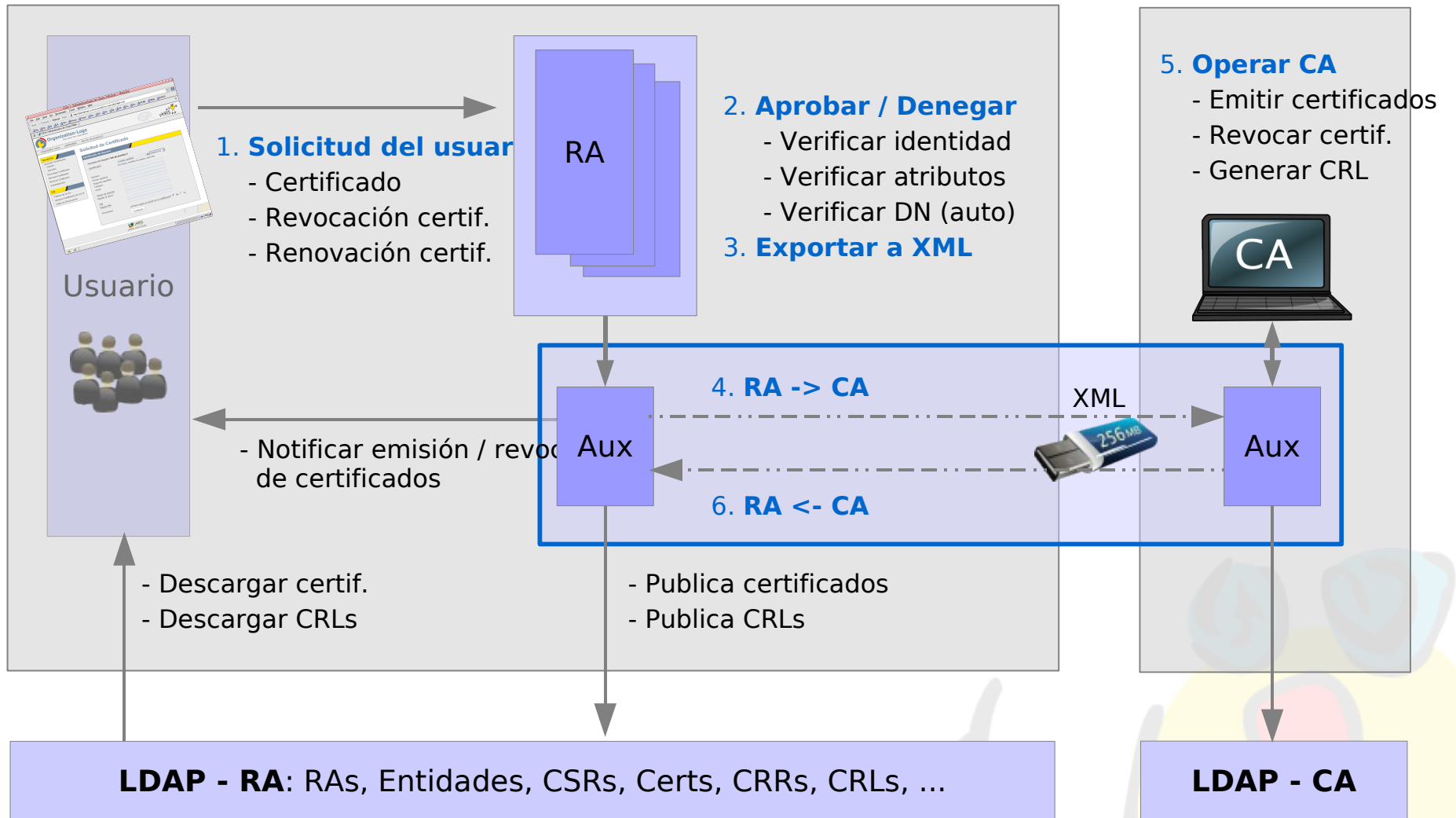
- Pruebas con diversos softwares de PKI
- Software de PKI demasiado complicado para nuestros requisitos

- Open SSL
- LDAP (pkIRIS schema)
 - Almacenar RAs, entidades, CSRs, certificados, logs, ...
- COPA
 - Codificación optimizada para acceso jerárquico a la información
 - a3b105c1 identifica a la RA 3, entidad 105 y CSR/cert 1
 - Errores
- URNs
 - Almacenar los estados en la vida de un certificado
 - urn:mace:rediris.es:cica.es:pkCICA:csr:state:20060714141456:new:10e19...2d6af7
- XML
 - Intercambio de ficheros entre CA y RAs
- PHP/JavaScript

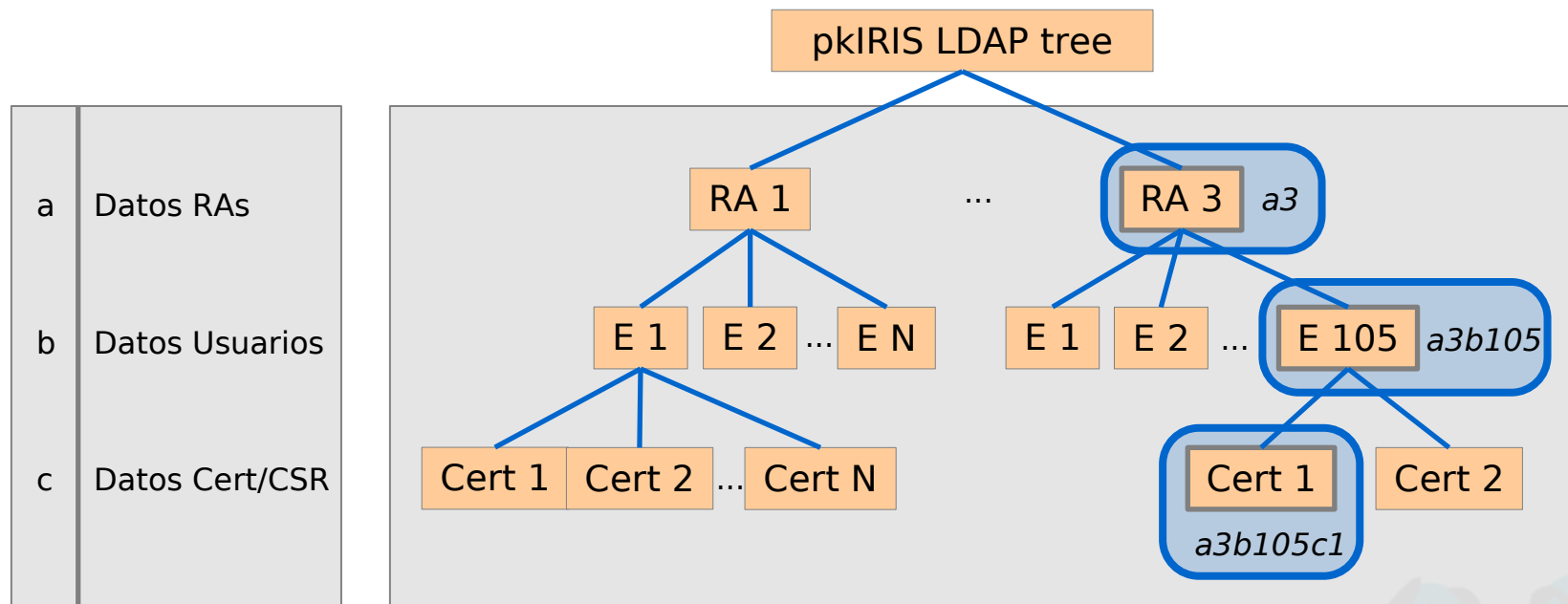
- **Público**
 - Política
 - Certificado CA
 - Certificados válidos
 - Lista de revocación
- **Usuarios**
 - Solicitud de certificados/renovaciones, revocaciones y descarga
- **RA**
 - Gestión de solicitudes (aprobación y denegación)
 - Exportación de datos a la CA (Generación de XML)
 - Revocación

- Operación PKI
 - Creación de RAs
 - Gestión de usuarios privilegiados
- CA
 - Gestión de solicitudes (emisión y denegación de certificados)
 - Traspaso de información
 - Emisión CRLS
 - Revocación

- **Solicitud de usuario**
 - certificado, renovación, revocación
- **Aprobación por el administrador RA**
 - identidad, atributos, responsabilidades
- **Exportación de solicitudes aprobadas a la CA**
- **Importación solicitudes por la CA**
 - emisión, denegación, revocación, CRLs
- **Exportación de la CA a la RA**
 - certificados, revocaciones, CRLs
- **Información a los solicitantes de los certificados**
- **Descarga de certificados (Comentario del navegador)**



Estructura lógica de la información



a3

identifica a la RA 3

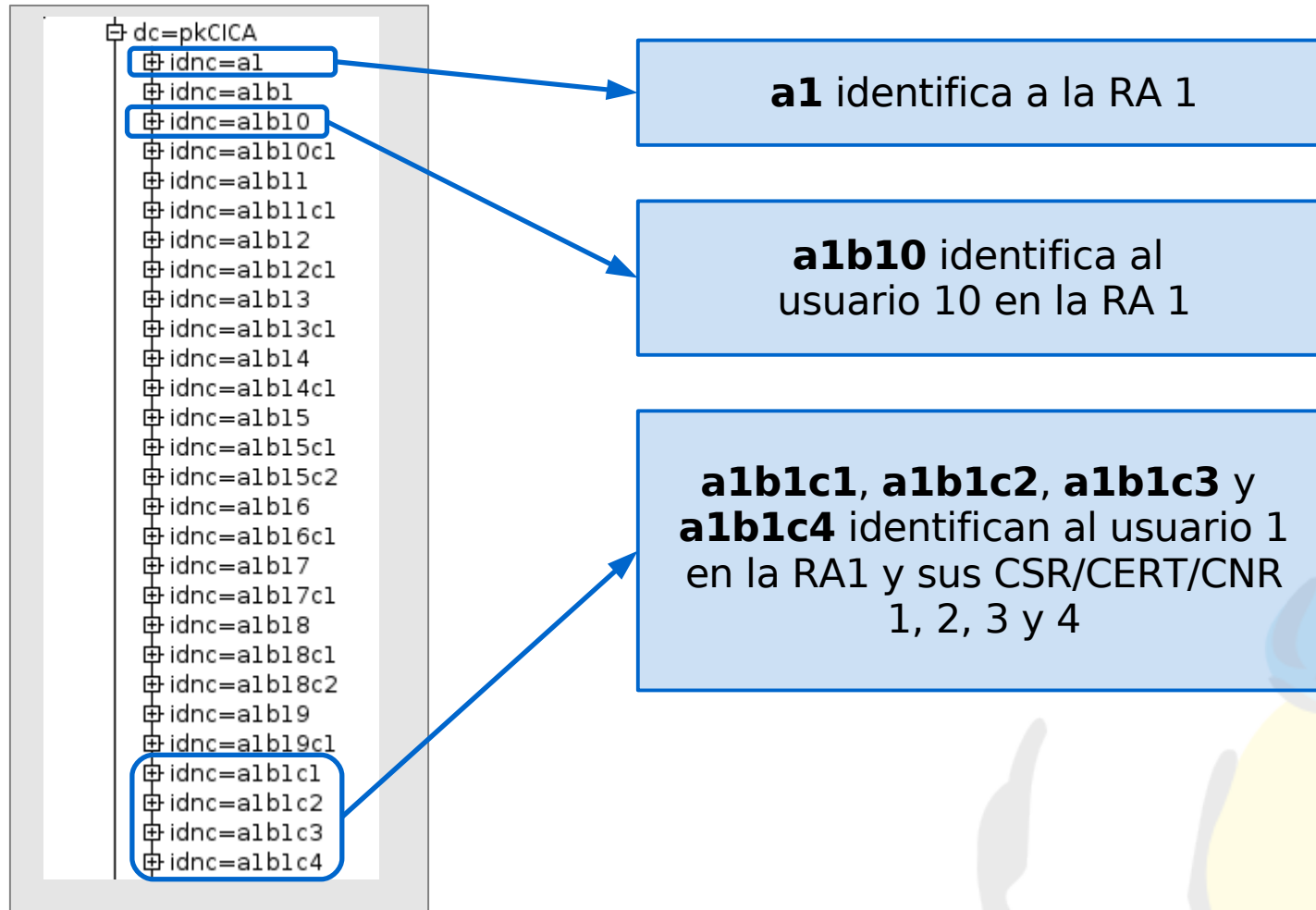
a3b105

identifica a la RA 3, entidad 105

a3b105c1

identifica a la RA 3, entidad 105, y certificado/CSR 1

Estructura física de la información



- **pkirisAuthority**

- pkirisID
- pkirisCopaID
- pkirisName
- pkirisRaUrl
- pkirisCounter

- **pkirisEndEntity**

- pkirisID
- pkirisCopaID
- pkirisCounter
- userPassword
- cn, sn, mail, ...

- **pkirisCertificate**

- pkirisID
- pkirisTrace
- pkirisStatus
- pkirisDate
- pkirisPin
- pkirisCSR
- pkirisRevocationReason
- pkirisRevokedByCopaID
- pkirisShowMail
- pkirisCertificateExpirationDate
- pkirisCertType
- pkirisCopaID
- pkirisSubjectDN
- userCertificate
- mail

dn	idnc=a1b1c4,dc=pkCICA,dc=cica,dc=es
objectClass	top pkirisCertificate
idnc	a1b1c4
irisClassifCode	
pkirisID	sebastian.balboa@cica.es
pkirisTrace	urn:mace:rediris.es:cica.es:pkICICA:csr:state:20060714134722:new:0581194297b2fd2f53f315a918956503e621 urn:mace:rediris.es:cica.es:pkICICA:csr:state:20060714141450:approved:6084c1da3990498b0206e2681843d3 urn:mace:rediris.es:cica.es:pkICICA:csr:state:20060714141456:ra2ca:beacca3cfae4960e080fb3cc0cc072430c urn:mace:rediris.es:cica.es:pkICICA:csr:state:20060714141805:csr-pending:39da5bfe90f2d973f9591fa43bd50a urn:mace:rediris.es:cica.es:pkICICA:csr:state:20060714141846:issued:4e20ddf944df4918a1d839d4103b3645e
pkirisStatus	issued
pkirisDate	20060714141846
pkirisPin	\$1\$oxWMn6qg\$ExRlmMGmu7b3.ayZknzei1
pkirisCSR	SPKAC=MICTDCCATQwggEiMA0GCSqSb3DQEBAQUAA4IBDwAwggEKAoIBAQQDY128LzZMoY8YqqVvb1mf7bmMSC
pkirisCertType	usr
pkirisCopalD	a1b1c4
userCertificate	MIIFwzCCBKugAwIBAgIBHzANBgkqhkiG9w0BAQUFADA8MRIwEAYKCCZImiZPyLGQBGRMCZX MxFDASBgoJkiaJk/IsZAEZEwRjajVhNAwDgYDVRQDEwdQSDSUNBMB4XDTA2MDcxNDEy MTgON1oXDTA3MDcxNDEyMTgON1owVDESMBAGCgmSJomT8ixkARkWAzMRQwEgYKCCZImiZ PyLGQBGRYEY21jYTEtMAsGA1UEChMEY21jYTEtMAsGA1UEAxMQc2ViYXN0aWZuLmJhbGJv YTCCAS1wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANANjXbvwNkyh.jxiqpXBvWZHu czdTnFPmubVy2xcHMk2+XLuA/8SEPUcr4M20oHk51rM1iGVCAId+CbjDE9E2avqKfbZB/9 s61njMcNz2wQF1Jp4eznbxRCqJ+skan6Q+BPqYX+PyXwinJ5T0159c0/NZTLn8cTRyaPbQ JC2+4wCq1XSvTgy01Cp0Q044eL+yxu0BsUtXwurrH9F7uWQNF3YugyWkM3yA6GJgWmUnh/T kx/xhI HRFnmFwKc2S5N i iNS+KvD/F 3uuRyZuYvD6/RChFS iSe TFce1lniN2TaAKK8u6 iZ0
pkirisSubjectDN	dc=es,dc=cica,o=cica,cn=sebastian.balboa
pkirisRevocationReason	
pkirisRevokedByCopalD	
pkirisShowMail	TRUE
pkirisCertificateExpirationDate	20070714121846
mail	sbalboa@cica.es

Cada operación sobre una CSR/Cert queda registrada mediante traza firmada, en un URN

CSR almacenada para un uso futuro

pkirisShowMail indica si el certificado llevará la dirección de correo o no

- Versiones

- Versión estable 0.95
- Desarrollo 0.96b

- Colaboradores

- Red Universitaria Nacional de Chile (REUNA)
- Universidad Nacional de Educación a Distancia (UNED) como betatesters
- Eva Masa (diseño logo)

- Descarga y participación

- Disponible en la Forja de RedIRIS.



<https://forja.rediris.es/projects/pkiris/>

- **Nuevas funcionalidades a corto plazo**
 - PAPI (Access control)
 - Utilización de csr generada externamente
 - Generación de múltiples CSRs
- **Nuevas funcionalidades a largo plazo**
 - Implementación en AJAX de la interfaz web
 - Módulo para la representación gráfica de la interfaz de usuario (XML)

**Muchas
gracias por
vuestra
atención**

