CICA RedIRIS

Jornadas Técnicas de RedIRIS
Granada, 16 noviembre 2006

pkIRIS

Una nueva forma de gestionar certificados

Sebastián Balboa García
sebastian.balboa@cica.es

Contenido

- ¿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

¿ Que es pkIRIS ?

- 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)

¿ Por que pkIRIS ?

- Requisitos
  - Distribución
    - lógica RAs (y física)
  - Simplicidad
    - Instalación del sistema
    - Creación de RAs
    - Gestión de RAs para administadores 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

Tecnología usada en pkIRIS

- 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

Módulos de pkIRIS

- 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

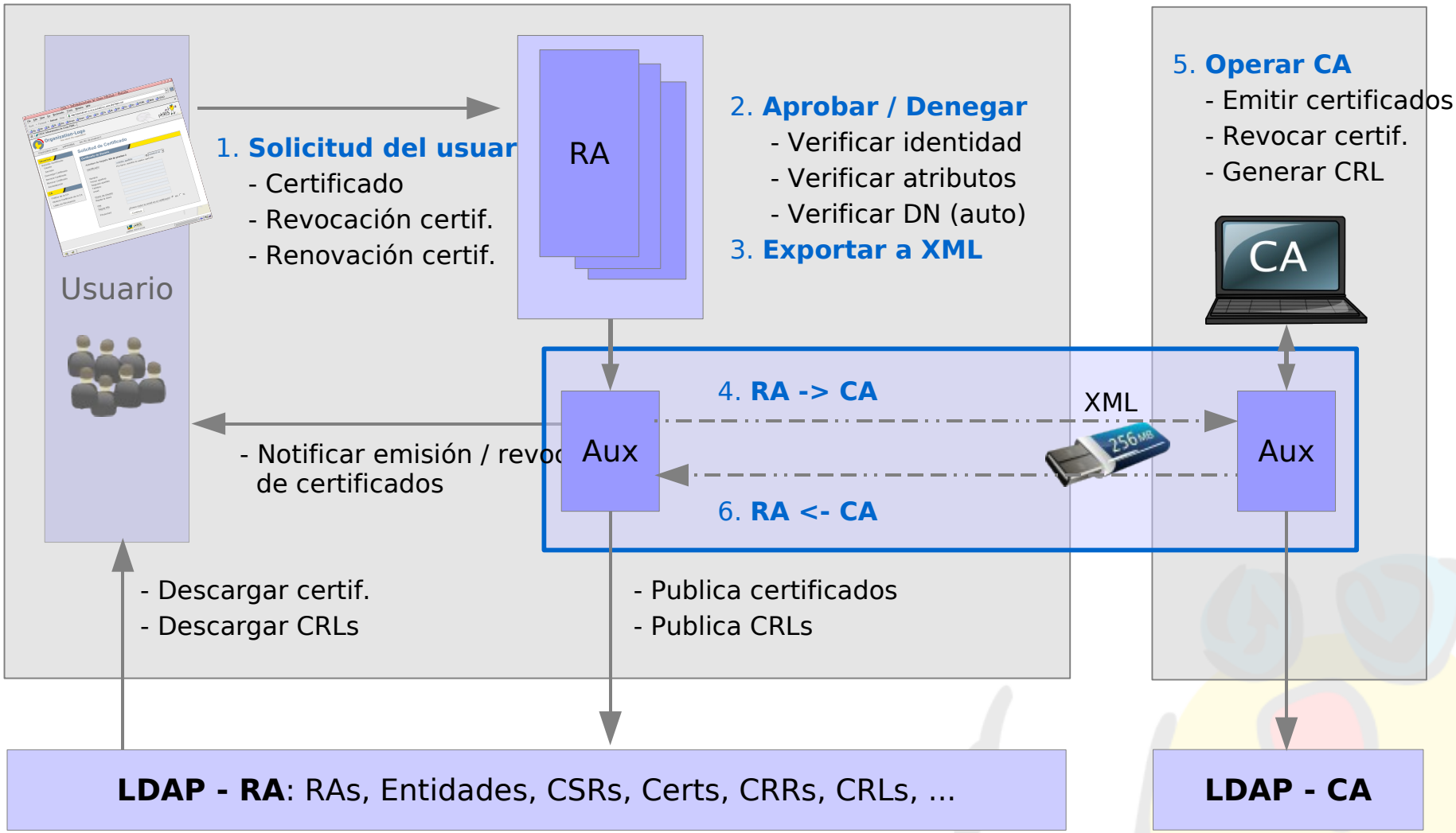
Módulos de pkIRIS

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

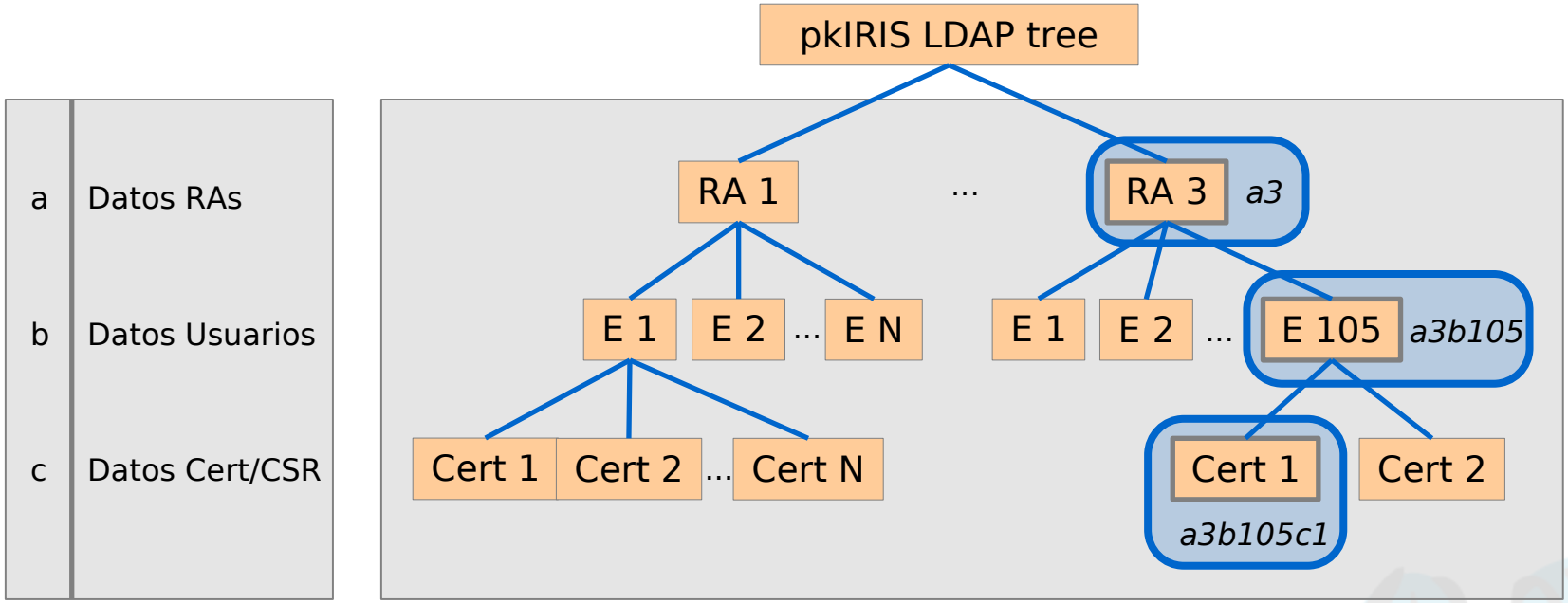
Flujograma de uso

- 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)

Flujograma gráfico

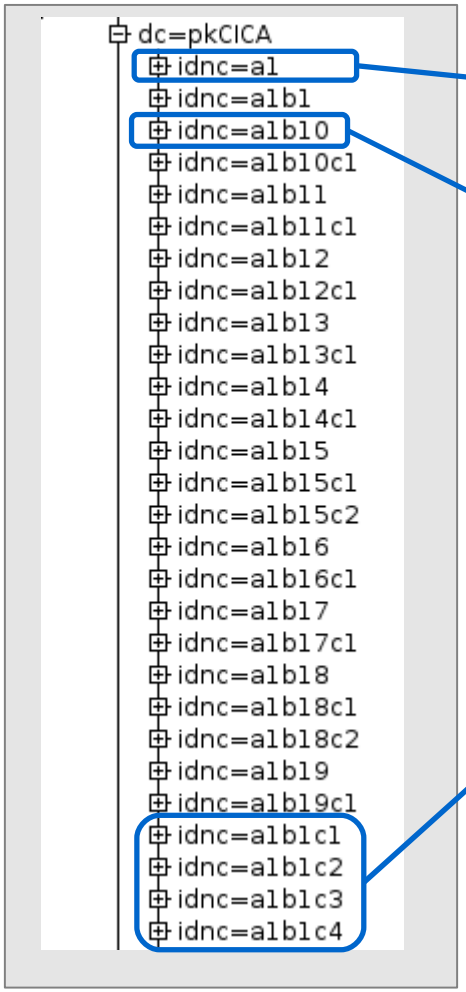


Estructura lógica de la información



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



a1 identifica a la RA 1

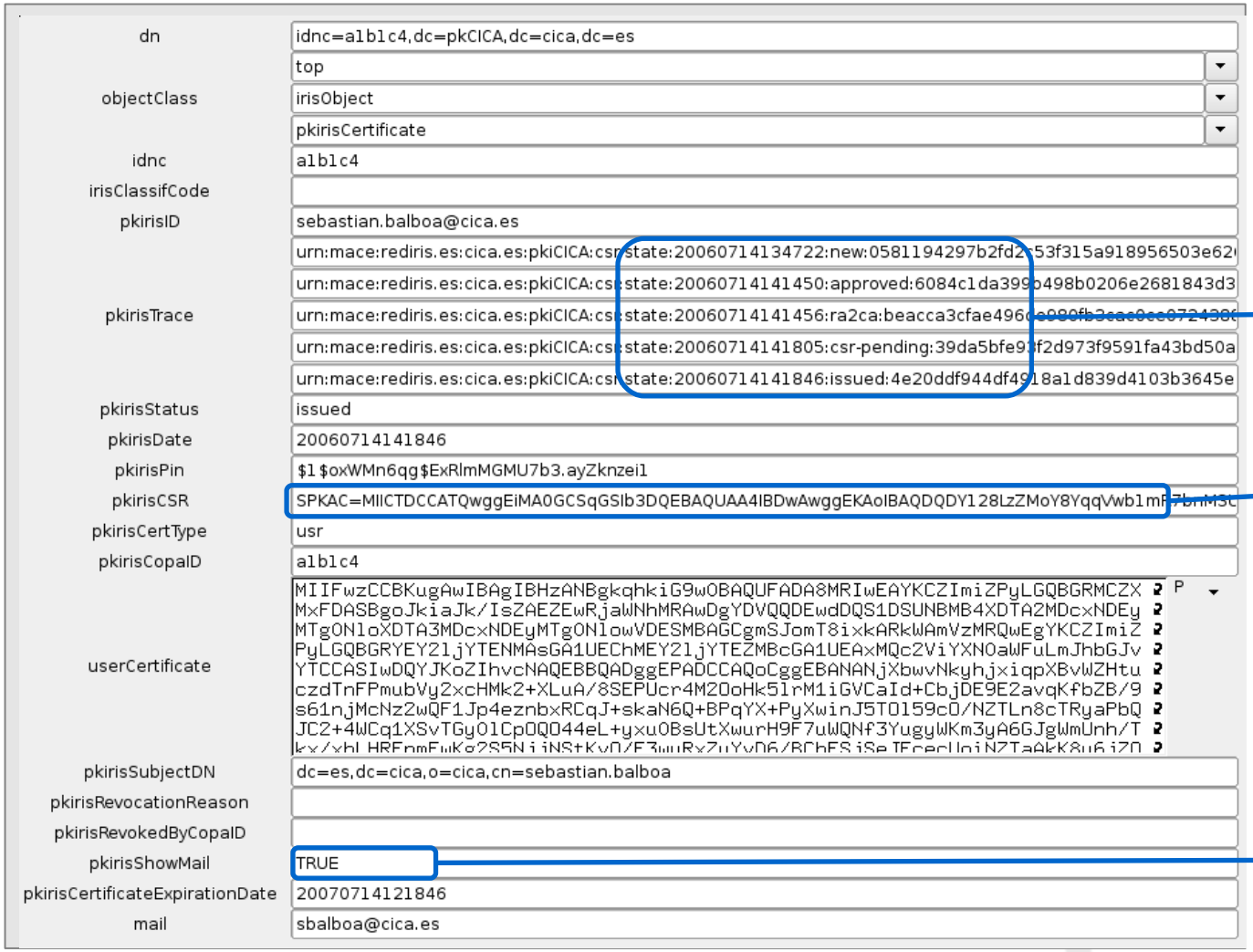
a1b10 identifica al usuario 10 en la RA 1

a1b1c1, **a1b1c2**, **a1b1c3** y **a1b1c4** identifican al usuario 1 en la RA1 y sus CSR/CERT/CNR 1, 2, 3 y 4

Esquema LDAP pkiris.schema

- **pkirisAuthority**
  - pkiris**ID**
  - pkiris**CopaID**
  - pkiris**Name**
  - pkiris**RaUrl**
  - pkiris**Counter**
- **pkirisEndEntity**
  - pkiris**ID**
  - pkiris**CopaID**
  - pkiris**Counter**
  - userPassword
  - cn, sn, mail, ...
- **pkirisCertificate**
  - pkiris**ID**
  - pkiris**Trace**
  - pkiris**Status**
  - pkiris**Date**
  - pkiris**Pin**
  - pkiris**CSR**
  - pkiris**RevocationReason**
  - pkiris**RevokedByCopaID**
  - pkiris**ShowMail**
  - pkiris**CertificateExpirationDate**
  - pkiris**CertType**
  - pkiris**CopaID**
  - pkiris**SubjectDN**
  - userCertificate
  - mail

Esquema LDAP pkiris.schema



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

Estado del proyecto

- 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/

Futuras versiones

- 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