Mauricio Campiglia

Hágalo Ud. Mismo:
Críe su propia PKI

Soluciones y repaso

- **Algoritmos de cifrado asimétrico**
  - Confidencialidad
  - Autenticidad
  - Integridad
  - ... dependiendo de cómo sea usado.
- **Problema de distribución de claves**
- **¿Qué es Firma digital?**
  - Hash cifrado... ¿simple no?

Paradigmas

- **Jerárquico**
  - Tercerización de la confianza (ya veremos qué confianza)
  - Requiere Autoridad Certificadora
  - Certificados tal como los conocemos (x.509)

  - Rapidez de crecimiento
  - Castillo de naipes

- **Entre Pares**
  - Confianza auto-administrada (trampas al solitario)

  - De lento crecimiento relativo
  - Malla de confianza

Usos del certificado

- Firma digital
- Validación de servicios
- Autentificación de personas
- Cifrado de datos
- Autentificación de acceso

Usos del certificado II

- Firma
- Cifrado
- Certificación

Componentes de una PKI

- **Registration Authority**
  - Es la base de la tercerización de la confianza
- **Certification Authority**
  - Quien firma los certificados
- **Validation Authority**
  - Vigencia y revocación (Clearing)
  - CRL, OCSP

OpenSSL

... y mucha voluntad

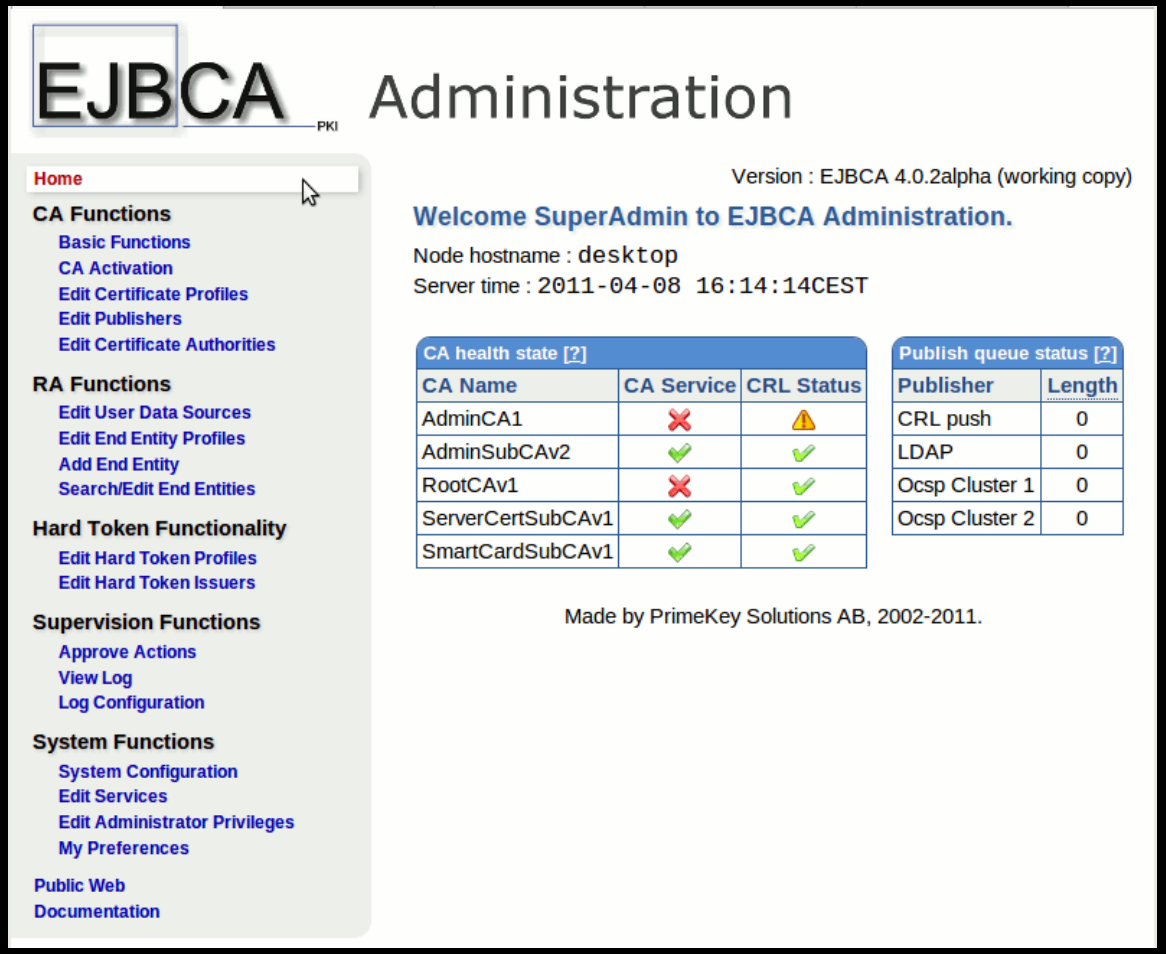
OpenCA

- **Gestión simplificada**
- **Web based**
- **Incluye los servicios necesarios:**
  - Registro
  - Firma
  - Validación
    - OCSP y CRL
- **Requerimientos:**
  - OpenSSL 0.9.7+
  - Apache Web Server
  - OpenCA-Tools
  - Base de datos (MySQL, PostgreSQL, DB2, Oracle)
  - PERL DBI

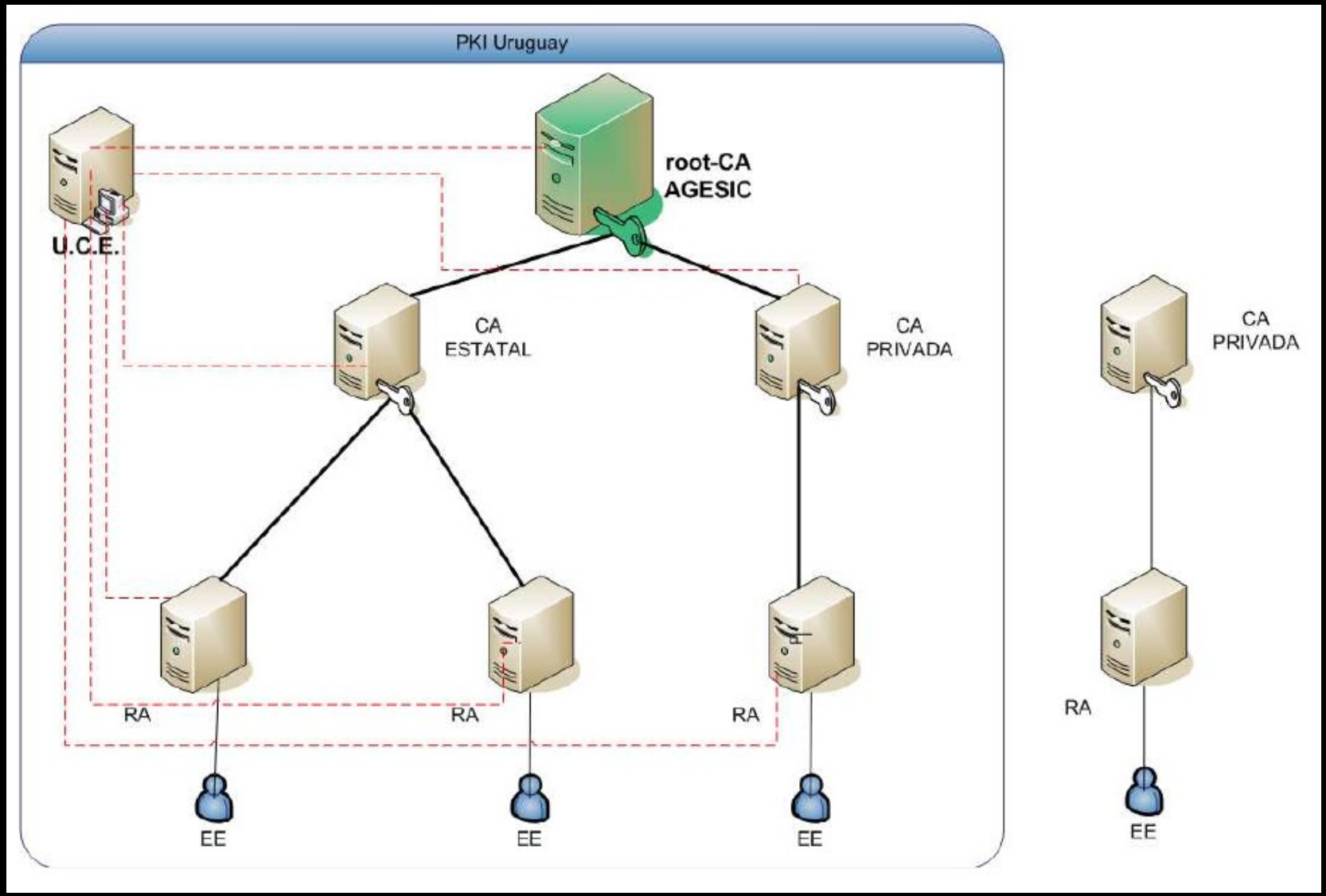
EJBCA

- Gestión simplificada alla Java
- Tiene requerimientos superiores a OpenCA

EJBCA



PKI Uruguay



Requisitos de seguridad

- **Seguridad física**
- **Equipo off-line**
- **HSM**
  - FIPS 140-2
- **Procesos, procesos, procesos**

¡Muchas Gracias!

¿Preguntas?

Mauricio Campiglia

mcampigl (at) uy (dot) ibm (dot) com
mauricio(at)campiglia.org