

Hágalo Ud. Mismo: Crée 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

*Autenticación de personas

*Cifrado de datos

*Autenticación 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

Administration

Version : EJBCA 4.0.2alpha (working copy)

[Home](#)

CA Functions

- [Basic Functions](#)
- [CA Activation](#)
- [Edit Certificate Profiles](#)
- [Edit Publishers](#)
- [Edit Certificate Authorities](#)

RA Functions

- [Edit User Data Sources](#)
- [Edit End Entity Profiles](#)
- [Add End Entity](#)
- [Search/Edit End Entities](#)

Hard Token Functionality

- [Edit Hard Token Profiles](#)
- [Edit Hard Token Issuers](#)

Supervision Functions

- [Approve Actions](#)
- [View Log](#)
- [Log Configuration](#)

System Functions

- [System Configuration](#)
- [Edit Services](#)
- [Edit Administrator Privileges](#)
- [My Preferences](#)

[Public Web](#)

[Documentation](#)

Welcome SuperAdmin to EJBCA Administration.

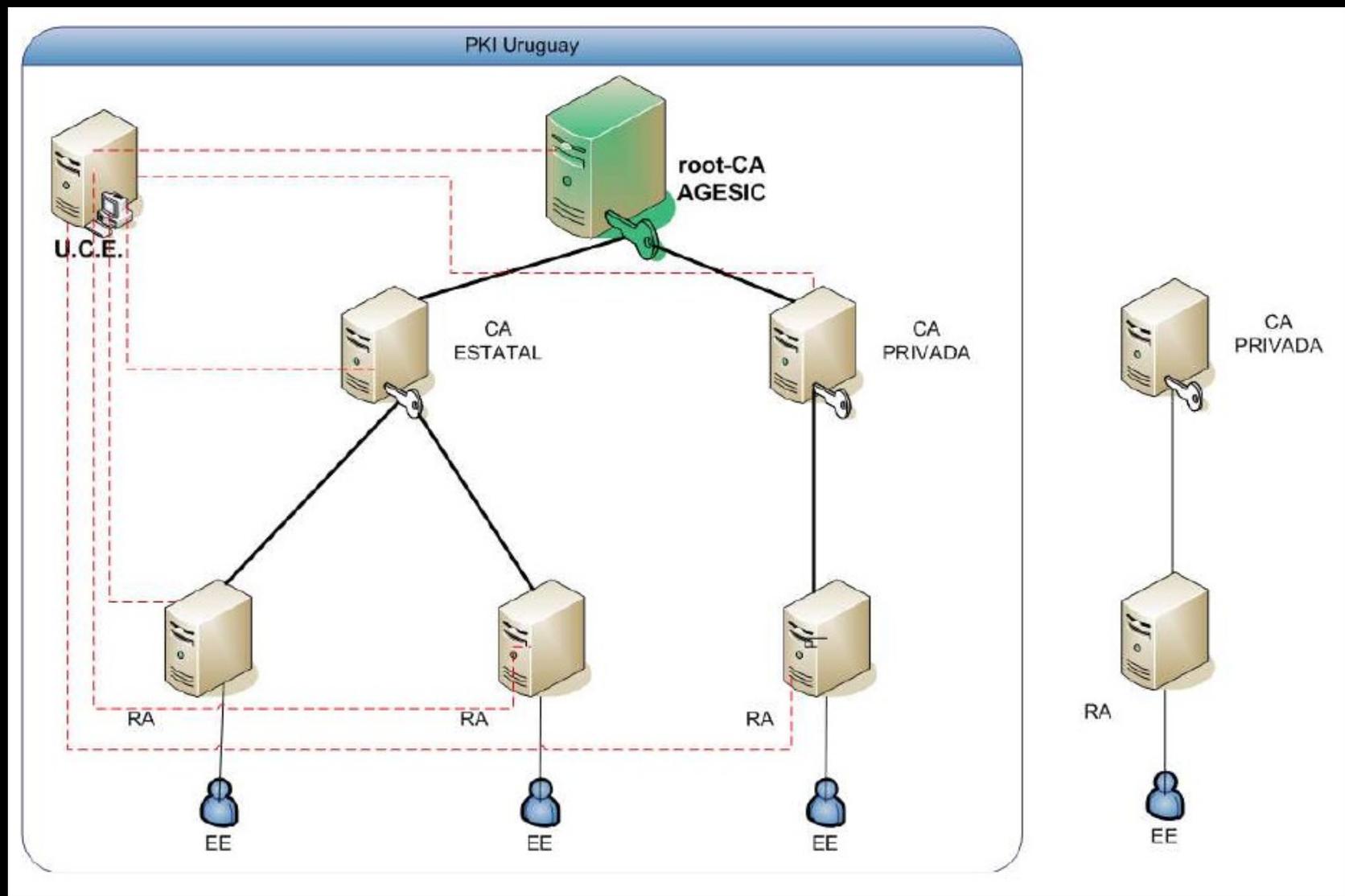
Node hostname : desktop
Server time : 2011-04-08 16:14:14CEST

CA health state [?]		
CA Name	CA Service	CRL Status
AdminCA1	✘	⚠
AdminSubCAv2	✔	✔
RootCAv1	✘	✔
ServerCertSubCAv1	✔	✔
SmartCardSubCAv1	✔	✔

Publish queue status [?]	
Publisher	Length
CRL push	0
LDAP	0
Ocsp Cluster 1	0
Ocsp Cluster 2	0

Made by PrimeKey Solutions AB, 2002-2011.

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