Introducción a las Infraestructuras de Clave Pública - PKI -

Miguel López Sánchez
Euskal Encounter 14

Índice

- Tecnología criptográfica
- Infraestructuras de clave pública
- Elementos criptográficos y contenedores
- Implementación real
- Utilidades y conclusiones
- Referencias

Tecnología criptográfica

Introducción

- Información = PODER

  ↓

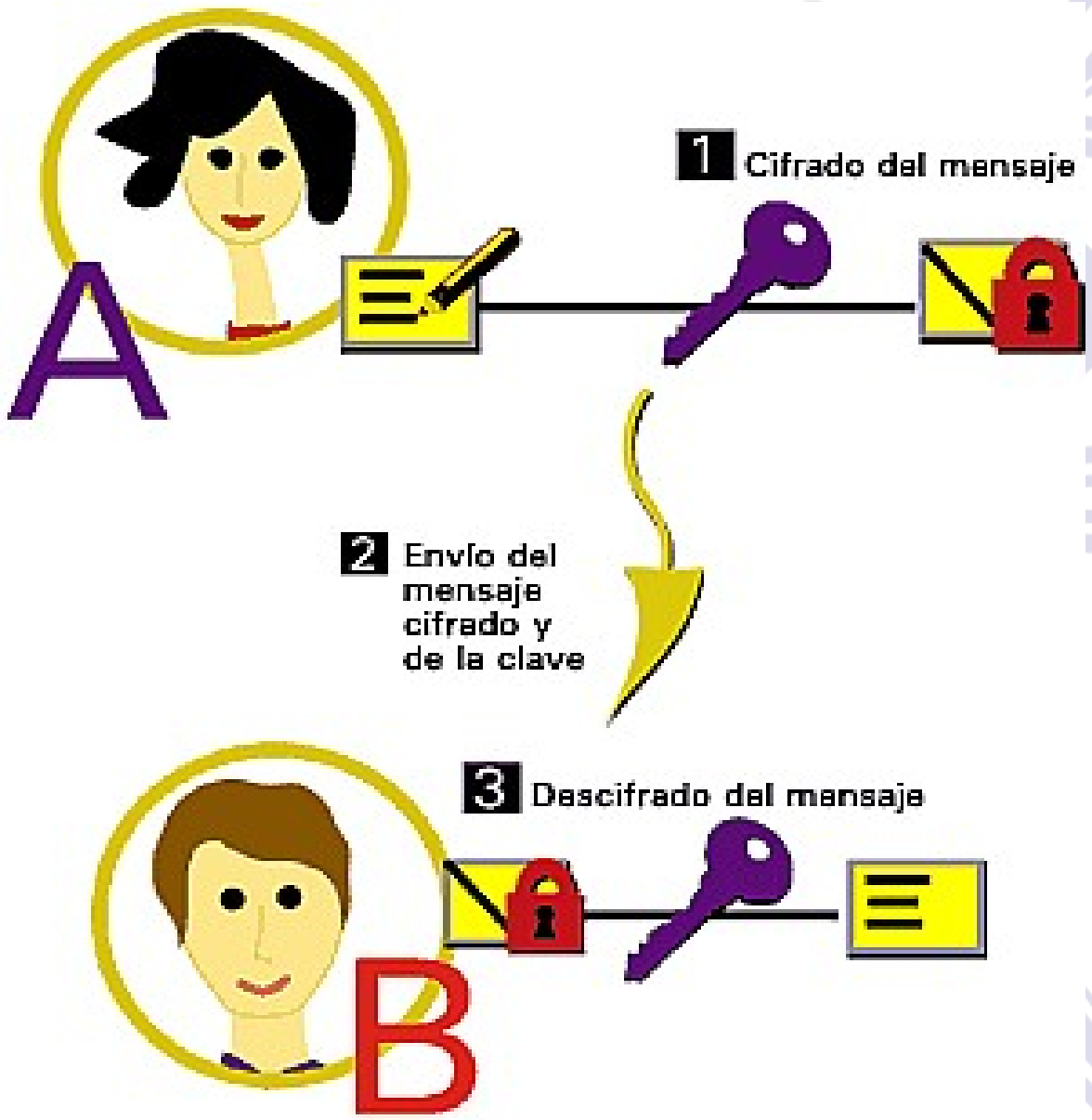
  Criptografía

- Requisitos de la seguridad
  - Confidencialidad
  - Disponibilidad
  - Integridad
  - Autenticidad
  - No repudio
- No existen los sistemas seguros

Cript. de clave simétrica (I)

- Una sola clave común = SECRETO
- Efectividad = Algoritmos + Longitud clave
- Dos grupos:
  - Cifradores de bloque
  - Cifradores de flujo
- Problemas:
  - Distribución de las claves
  - Gestión de claves
- Algoritmos: DES, 3-DES, AES, IDEA, RC6,...

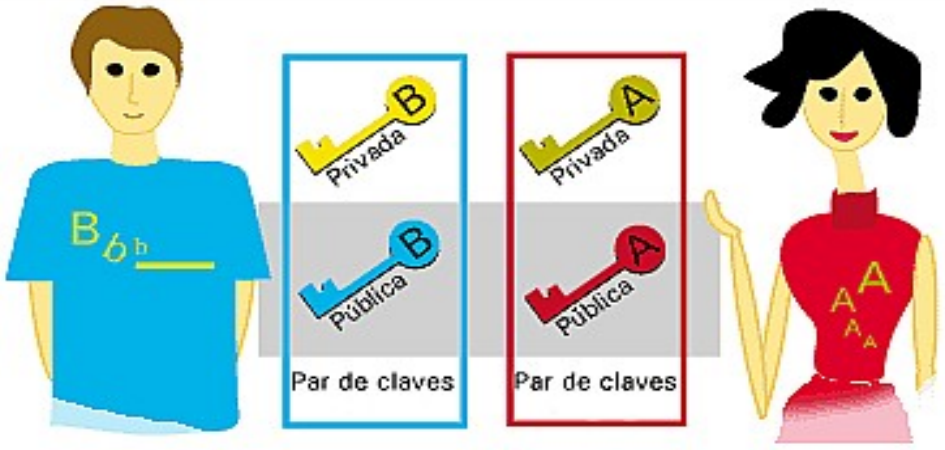
Cript. de clave simétrica (II)

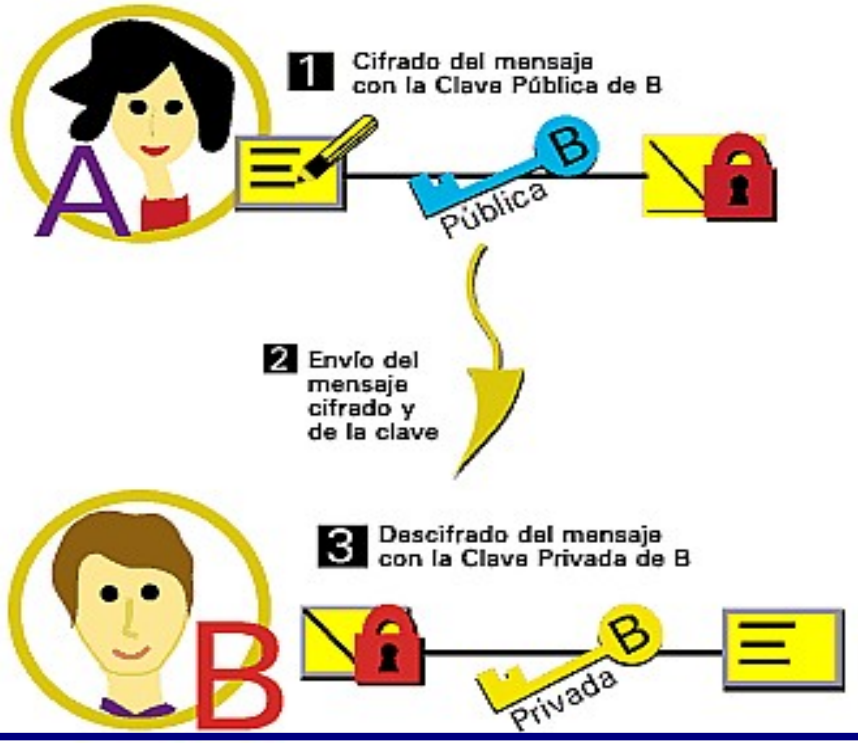


Cript. de clave asimétrica (I)

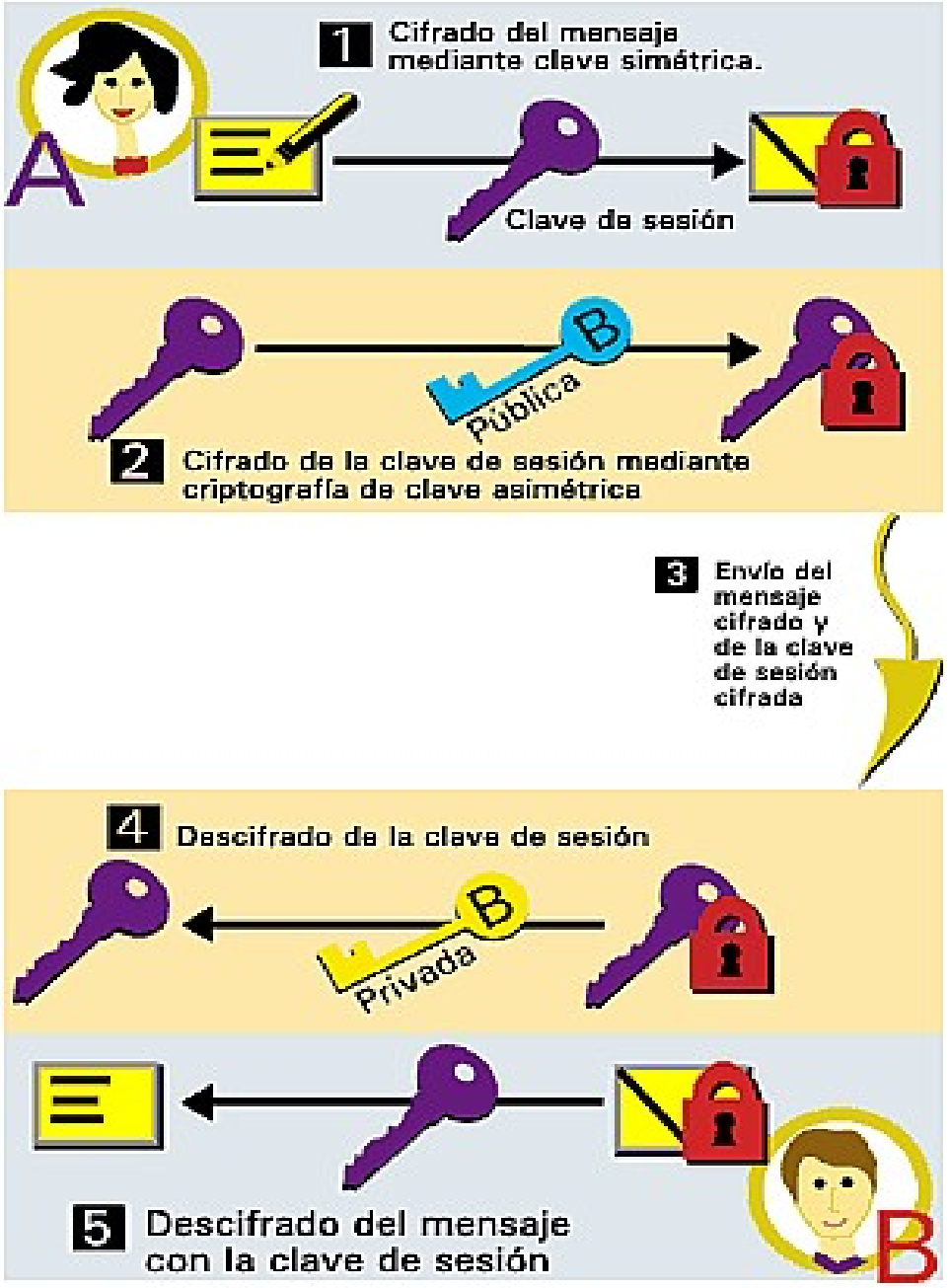
- Un par de claves complementarias
  - Pública (Kpub) + Privada (Kpriv)
- Efectividad: Costes computacionales
- 2 posibilidades
  - Autenticación ▸ $D_{Kpub}[C_{Kpriv}[m]]$
  - Confidencialidad ▸ $D_{Kpriv}[C_{Kpub}[m]]$
- Problemas: Cifrado lento
- Algoritmos: RSA, ECC, ElGamal, DSA,...

Cript. de clave asimétrica (II)





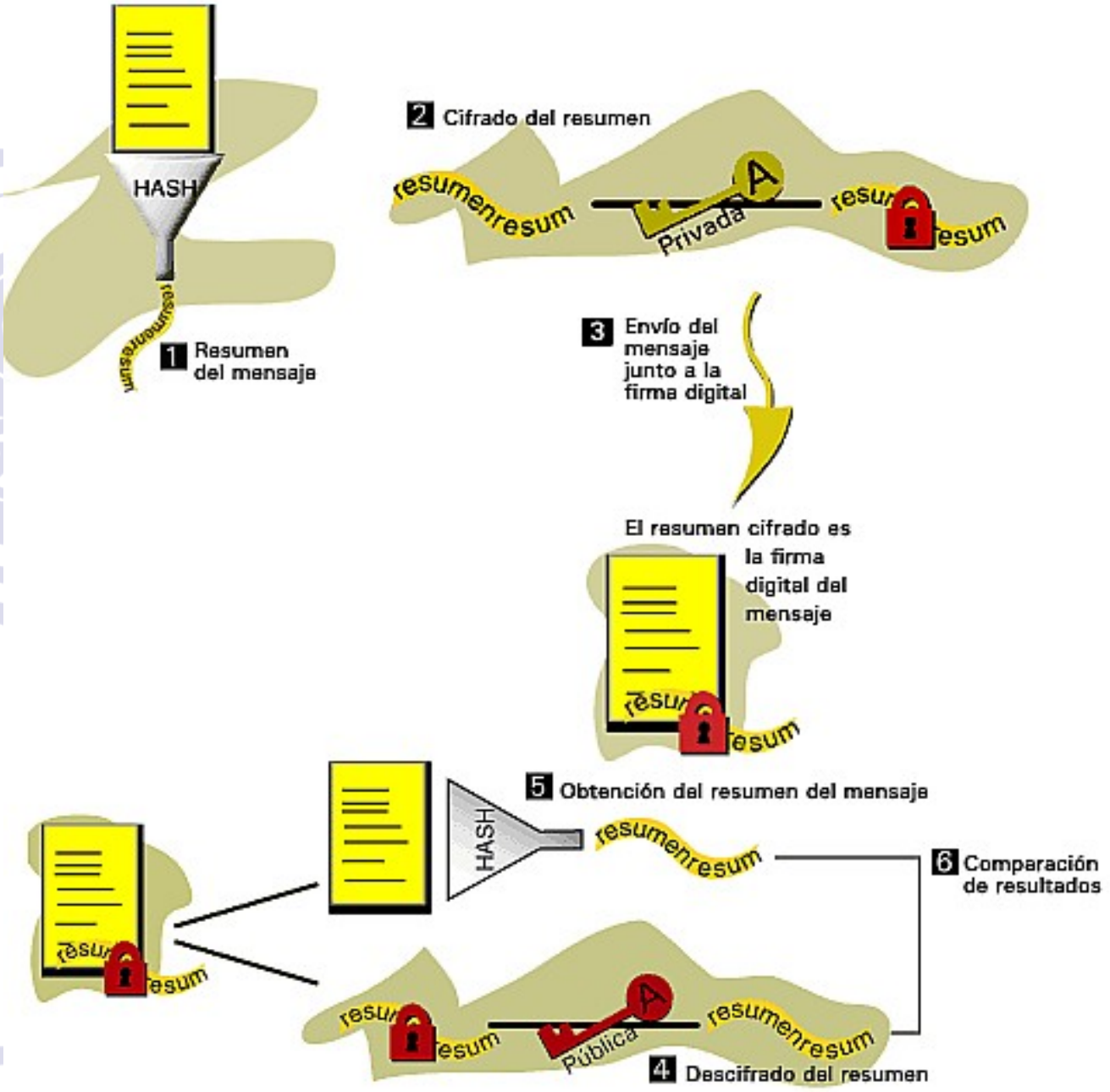
Cript. simétrica + asimétrica



Hash / MAC

- Funciones unidireccionales (NO REVERSIBLE)
- Resumen de tamaño fijo
- Hash ▸ Hash=h[m]
  - Integridad
  - SHA-1, MD-5, Whirlpool...
- MAC ▸ MAC=f[k,m]
  - Autenticidad + Integridad
  - HMAC

Firma Digital



Certificados Digitales (I)

- Aseguran ▸ Clave pública = usuario
- Información principal:
  - Emisor
  - Titular
  - Firma
  - Periodo de validez
  - Clave pública
  - Algoritmos utilizados
- Estado de los certificados:
  - Activo o preactivo
  - Suspendido
  - Revocado
- Estándar X.509v3

Certificados Digitales (II)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: emailAddress=email,CN=NOMBRE,OU=UNIDAD ORGANIZATIVA,O=ORGANIZACIÓN,C=ES
        Validity
            Not Before: Jul 19 11:32:10 2006 GMT
            Not After : Jul 18 11:32:10 2008 GMT
        Subject: serialNumber=1,CN=ROL,OU=UNIDAD ORGANIZATIVA,O=ORGANIZACIÓN,C=ES
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:d5:c0:41:13:d7:a0:fa:dd:28:55:81:0c:bf:57:
            [...]
                    30:6d:ca:44:d9:42:94:38:12:7e:32:fb:ed:1e:ef
                Exponent: 65537 (0x10001)
            [...]
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            [...]
            X509v3 Subject Key Identifier:
                9E:7D:99:D9:0F:42:C2:17:CA:2B:9D:6B:DB:DD:A4:EE:E7:82:1C:2A
            X509v3 Authority Key Identifier:
                keyid:E2:7E:63:C7:18:67:EA:B1:BF:4B:61:85:3D:64:45:0A:9A:D9:3E:D3
            [...]

    Signature Algorithm: sha1WithRSAEncryption
        58:e8:93:c2:b0:44:30:70:5a:11:8d:03:db:8d:54:4a:78:5e:
        [...]
        89:df:f4:1c:c5:07:8f:54
-----BEGIN CERTIFICATE-----
MIIHtjCCBZ6gAwIBAgIBATANBgkqhkiG9w0BAQUFADCBqzELMAkGA1UEBhMCRVMx
[...]
w+iJ3/QcxQePVA==
-----END CERTIFICATE-----
```

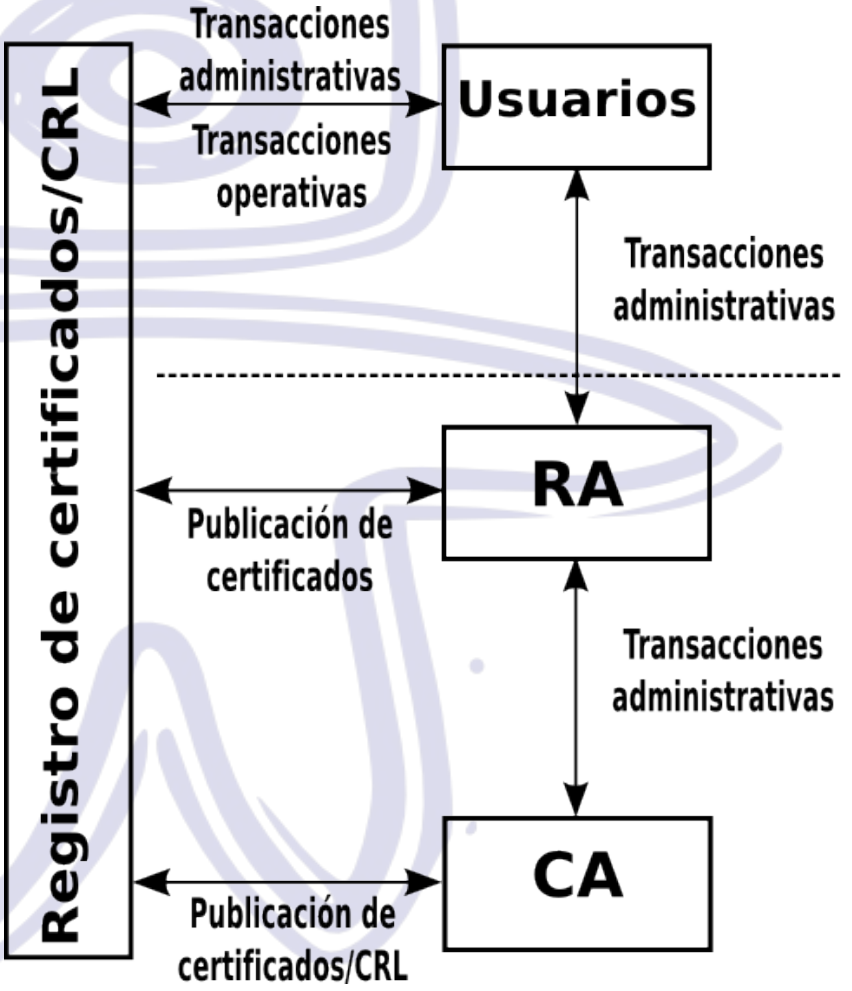
Infraestructura de Clave Pública

Estructura

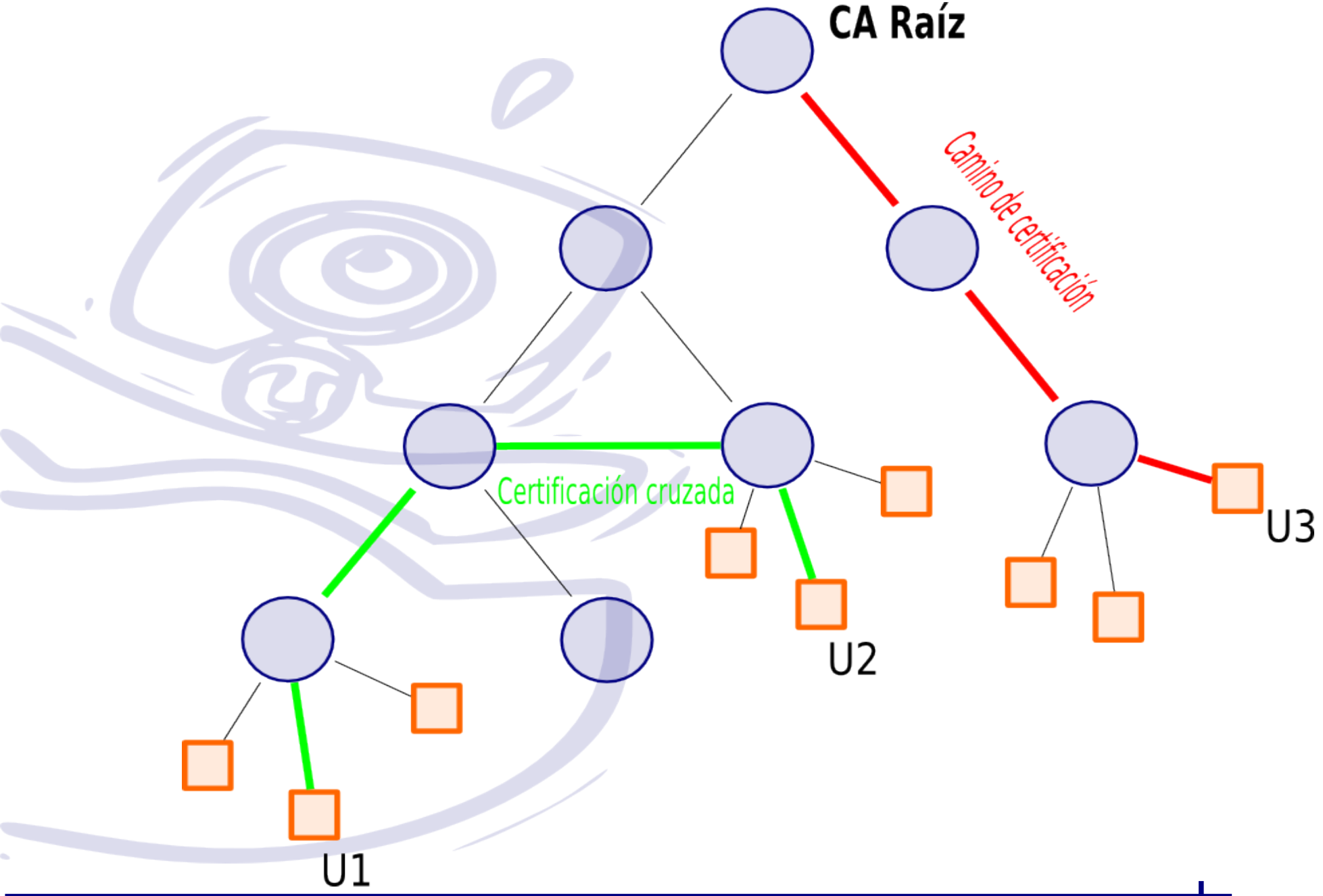
- HW + SW + Políticas + Procedimiento

  ASEGURAR LA IDENTIDAD

- Componentes
  - Usuarios/Clientes
  - Autoridad de Certificación
  - Autoridad de Registro
  - Repositorio
    - Certificados
    - CRL
  - Autoridad de sellado temporal



Red de confianza



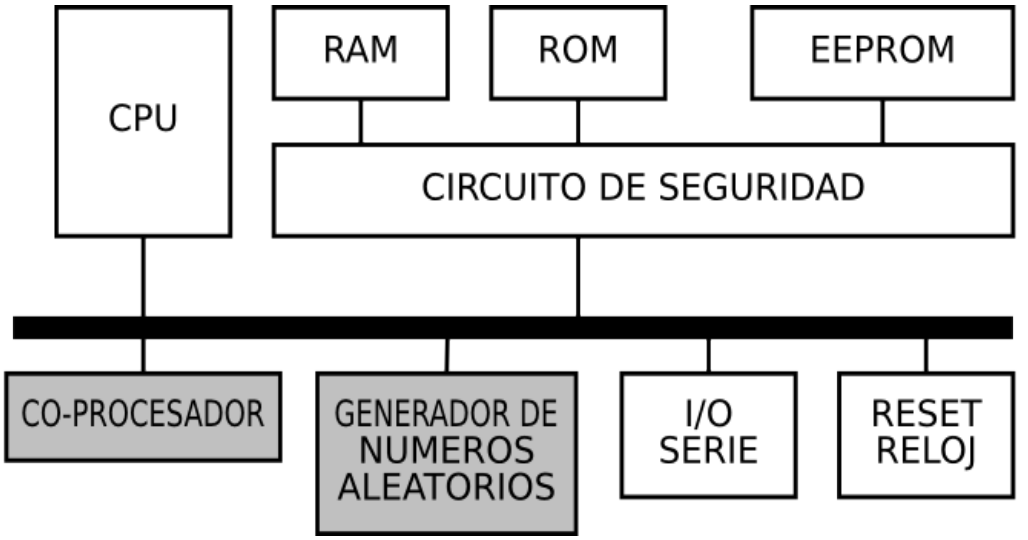
PKCS

Resumen de los estándares PKCS		
	Versión	**Nombre**
PKCS#1	2,1	Estándar criptográfico RSA
PKCS#2	-	*Obsoleto*
PKCS#3	1,4	Estándar de intercambio de claves Diffie-Hellman
PKCS#4	-	*Obsoleto*
PKCS#5	2	Estándar de cifrado basado en contraseñas
PKCS#6	1,5	Estándar de sintaxis de certificados extendidos
PKCS#7	1,5	Estándar sobre la sintaxis del mensaje criptográfico
PKCS#8	1,2	Estándar sobre la sintaxis de la información de clave privada
PKCS#9	2	Tipos de atributos seleccionados
PKCS#10	1,7	Estándar de solicitud de certificación
PKCS#11	2,2	Interfaz de dispositivo criptográfico (cryptoki)
PKCS#12	1	Estándar de sintaxis de intercambio de información personal
PKCS#13	–	Estándar de criptografía de curva elíptica
PKCS#14	–	Generación de número pseudo-aleatorios
PKCS#15	1,1	Estándar de formato de información de dispositivo criptográfico

Elemento criptográficos y contenedores

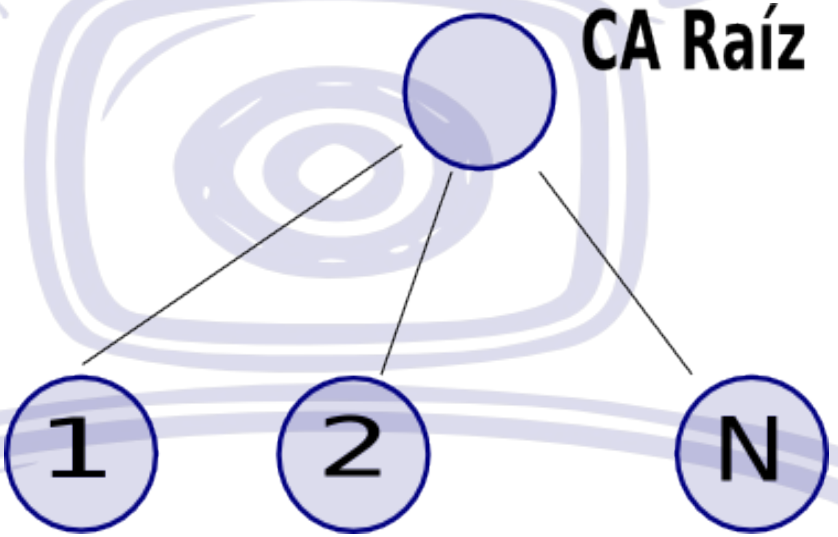
CSU / Tarjetas / Tokens

- Características
  - Creación de claves
  - Almacenamiento
  - Op. criptográficas
  - Portabilidad
- Acceso PKCS#11
- Contenido PKCS#15
- Certificaciones
  - Common criteria (ISO 15408)
- Contenedores SW



DNI-e (I)

- 2 años de despliegue
- Contenido del DNI-e:
  - Datos de filiación
  - Fotografía
  - Firma manuscrita
  - Impresiones dactilar
  - Par de claves ▸ FIRMA
  - Par de claves ▸ IDENTIDAD
- Acceso mediante PIN (8 dígitos)
- PKCS#11



DNI-e (II)

- DN [issuer name]:

```
CN= AC DNIE XXX

OU=DNIE

O=DIRECCIÓN GENERAL DE LA POLICÍA

C=ES
```

- DN [subject name]:

```
CN=<APELLIDO1> <APELLIDO2>, <NOMBRE>
   (AUTENTICACIÓN|FIRMA)

GN=<NOMBRE>

SN=<APELLIDO1>

NÚMERO DE SERIE=<DNI>

C=ES
```

- Contenido UTF-8
- Algoritmo: RSA
- Longitud módulo:
  - CA Raíz: 4096
  - CA Sub y Usuarios: 2046
- Hash: SHA-1/SHA-256

Implementación real

Alternativas y entorno

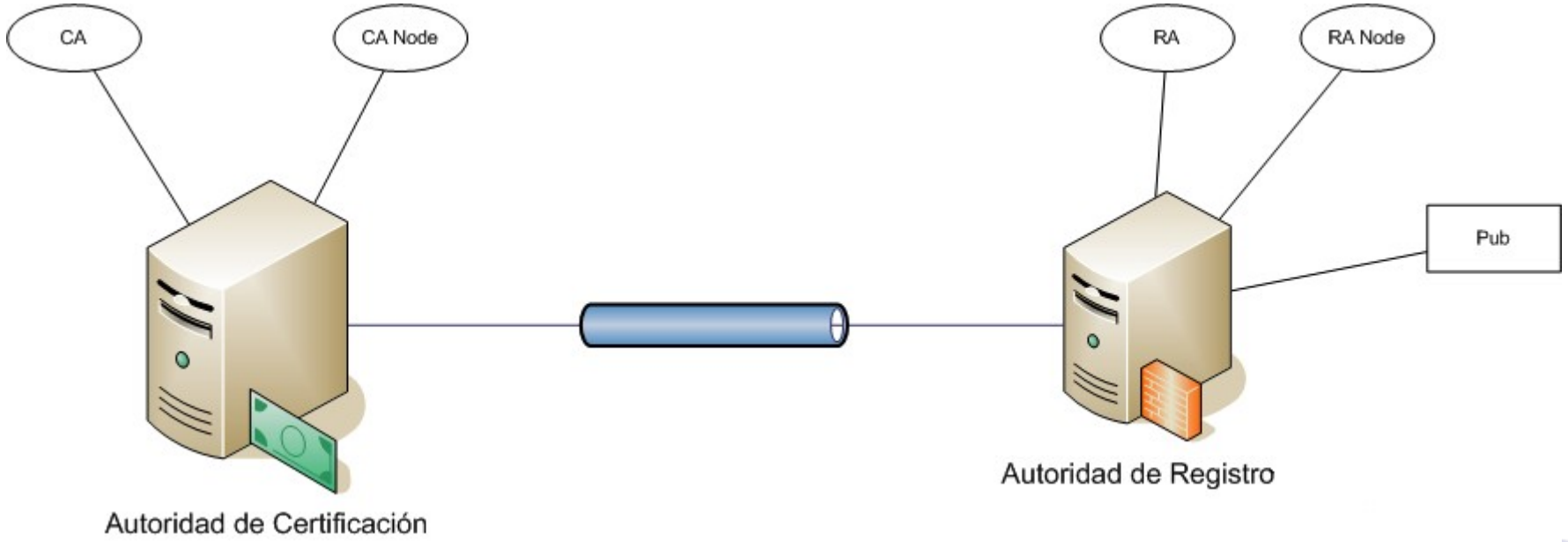
- Entorno
  - Desconocimiento
  - Desconfianza
  - Desestandarización
  - Ocultismo
- Implementaciones
  - Entrust
  - OpenSSL
  - RSA Security
  - Openca
  - Netscape CMS
  - Safelayer
  - TinyCA

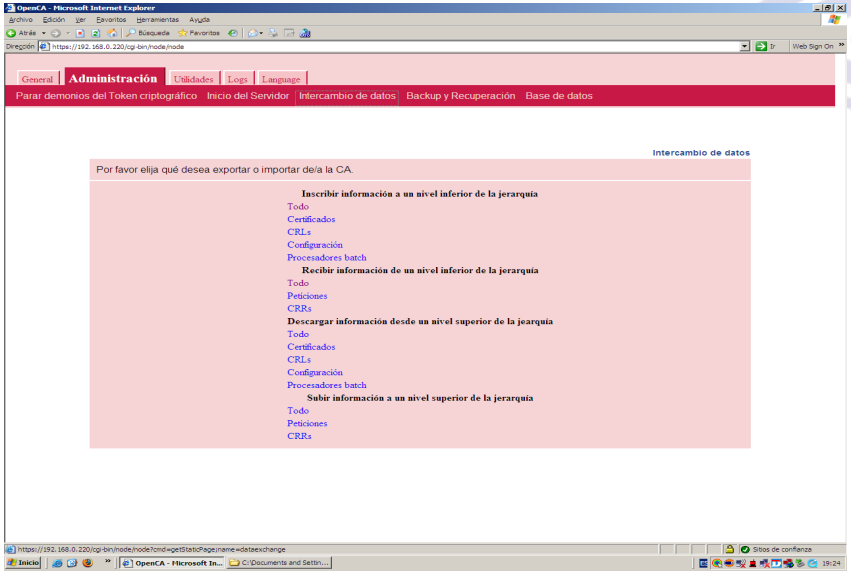
OpenCA (I)

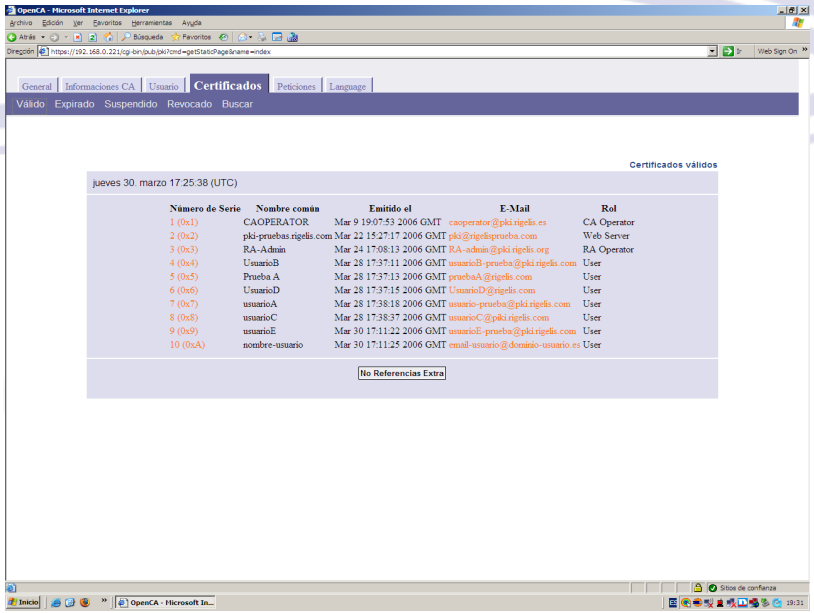
- Infraestructura completa PKI
- S.O.: BSD, Linux
- Software Libre
- Escrita en Perl
- Versión: 0.9.2.5
- Sobre OpenSSL
- Característica:
  - Múltiples configuraciones
  - Configuración XML
  - Multidioma (UTF8)

OpenCA
Research & Development Labs

OpenCA (II)

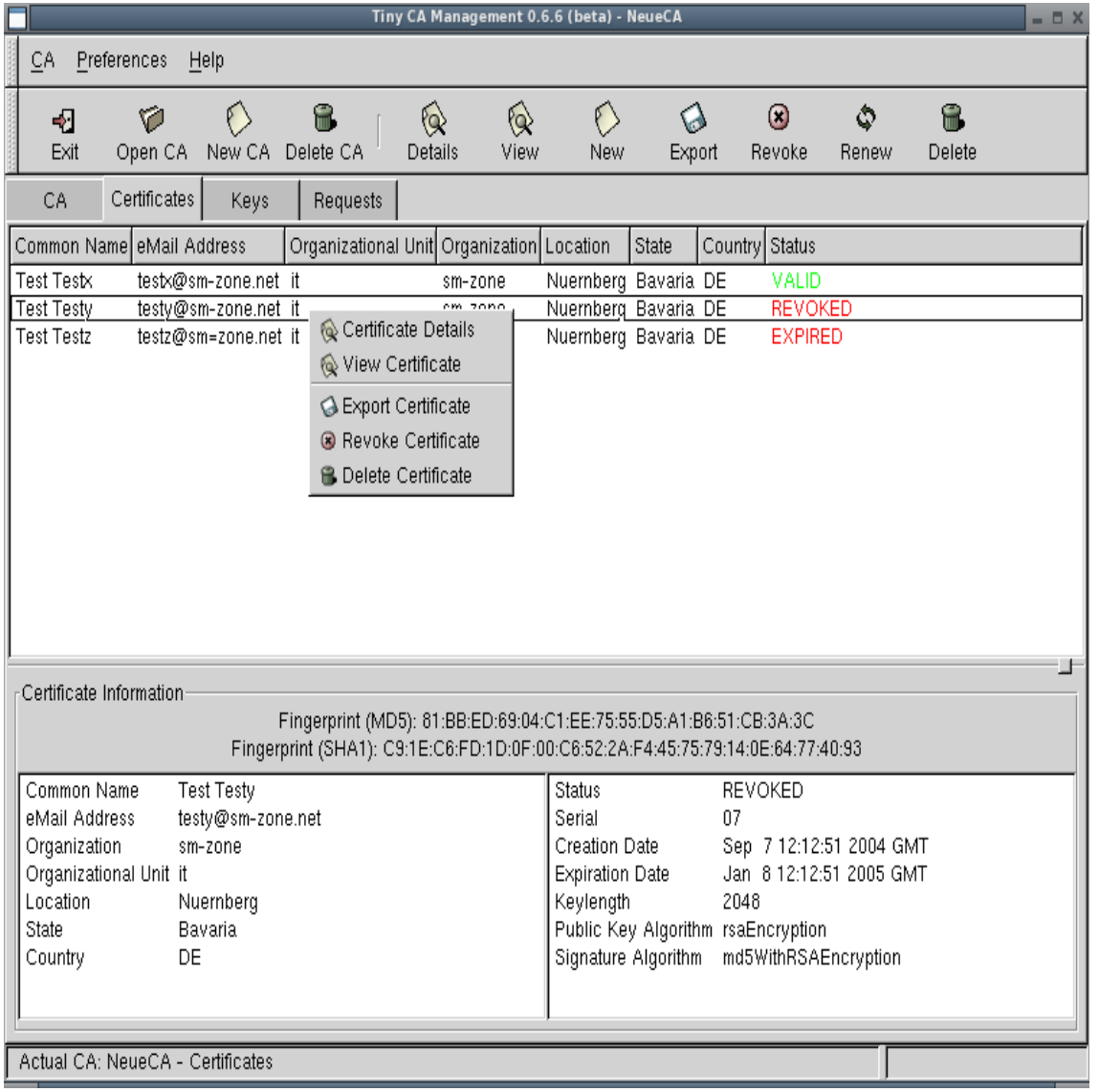

CA
CA Node
RA
RA Node
Pub
Autoridad de Certificación
Autoridad de Registro


OpenCA - Microsoft Internet Explorer
General
Administración
Utilidades
Logs
Language
Parar demonios del Token criptográfico
Inicio del Servidor
Intercambio de datos
Backup y Recuperación
Base de datos
Intercambio de datos
Por favor elija qué desea exportar o importar de/a la CA.
Inscribir información a un nivel inferior de la jerarquía
Todo
Certificados
CRLs
Configuración
Procesadores batch
Recibir información de un nivel inferior de la jerarquía
Todo
Peticiones
CRRs
Descargar información desde un nivel superior de la jearquía
Todo
Certificados
CRLs
Configuración
Procesadores batch
Subir información a un nivel superior de la jerarquía
Todo
Peticiones
CRRs


OpenCA - Microsoft Internet Explorer
General
Informaciones CA
Usuario
Certificados
Peticiones
Language
Válido
Expirado
Suspendido
Revocado
Buscar
Certificados válidos
jueves 30 marzo 17:25:38 (UTC)
Número de Serie
Nombre común
Emitido el
E-Mail
Rol
1 (0x1) CAOPERATOR Mar 9 19:07:53 2006 GMT caoperator@pki.rigelis.es CA Operator
2 (0x2) pki-pruebas.rigelis.com Mar 22 15:27:17 2006 GMT pki@rigelisprueba.com Web Server
3 (0x3) RA-Admin Mar 24 17:08:13 2006 GMT RA-admin@pki.rigelis.org RA Operator
4 (0x4) UsuarioB Mar 28 17:37:11 2006 GMT usuarioB-prueba@pki.rigelis.com User
5 (0x5) Prueba A Mar 28 17:37:13 2006 GMT pruebaA@rigelis.com User
6 (0x6) UsuarioD Mar 28 17:37:15 2006 GMT UsuarioD@rigelis.com User
7 (0x7) usuarioA Mar 28 17:38:18 2006 GMT usuario-prueba@pki.rigelis.com User
8 (0x8) usuarioC Mar 28 17:38:37 2006 GMT usuarioC@piki.rigelis.com User
9 (0x9) usuarioE Mar 30 17:11:22 2006 GMT usuarioE-prueba@pki.rigelis.com User
10 (0xA) nombre-usuario Mar 30 17:11:25 2006 GMT email-usuario@dominio-usuario.es User
No Referencias Extra

TinyCA / roCA

- TinyCA
  - Frontal de OpenSSL
  - Perl/GTK2
  - Versión 0.7.4
- roCA
  - Live-CD (Knoppix)
  - Almacenamiento USB
  - Versión 0.2.1



Utilidades y conclusiones

Utilidades y conclusiones

- Ámbitos
  - VPNs
  - Servicios Web
  - Firmado de documentación
  - Login
  - Redes Wifi
- Beneficios
  - Aumento de la seguridad
  - Agilización de operaciones
  - Mayor comodidad

Referencias

Referencias

- Aladdin, *Aladdin Knowledge Systems – Software security, Internet security, content filtering, Software D*, disponible en Internet. (http://www.aladdin.com/) (21 julio 2006)
- Alarcos, B., *Transporte de datos*, disponible en Internet. (http://it.aut.uah.es/alarcos/) (21 julio 2006)
- CERES, *CERES. FNMT-RCM*, disponible en Internet. (http://www.cert.fnmt.es/) (21 julio 2006)
- C3po, *C3PO: diseño y fabricación de lectores de tarjeta inteligente*, disponible en Internet. (http://www.c3po.es/) (21 julio 2006)
- De la Hoz, E., *Seguridad en Internet – Ingeniería en Informática*, disponible en Internet. (http://it.aut.uah.es/enrique/docencia/ii/seguridad/) (21 julio 2006)
- DNI electrónico, *Portal Oficial sobre el DNI electrónico*, disponible en Internet. (http://www.dnielectronico.es/) (21 julio 2006)
- Entrust, *Entrust – Strong Authentication, Real Time Fraud Detection, Protecting Information, SSL Certification*, disponible en Internet. (http://www.entrust.com/) (21 julio 2006)
- Kriptópolis, *kriptópolis.com*, disponible en Internet. (http://www.kriptopolis.com/) (21 julio 2006)
- López, M. (2005). *Registro público con infraestructura de clave pública*. PFC Universidad de Alcalá, Escuela Politécnica Superior.
- Lucena, M. J. (2006). *Criptografía y Seguridad en Computadores*. 4ª Edición. Club Universitario.

Referencias

- Master, D. (2004), *Criptosistemas Informáticos*, disponible en Internet. (http://sigt.net/wp-content/uploads/Criptosis.pdf) (21 julio 2006).
- Nash, A., Duane, W., Joseph, C. y Brink, D. (2002). *PKI Infraestructura de claves públicas. La mejor tecnología para implementar y administrar la seguridad electrónica de su negocio*. McGraw-Hill.
- Navas, P (2006). *Sistema de Autentificación de Redes inalámbricas basada en criptografía de clave pública*. PFC Universidad de Alcalá, Escuela Técnica Superior de Ingeniería Informática.
- OpenCA, *OpenCA Labs*, disponible en Internet. (http://www.openca.org/) (21 julio 2006)
- OpenSSL, *OpenSSL: The Open Source toolkit for SSL/TLS*, disponible en Internet (http://www.openssl.org/) (21 julio 2006)
- RoCA, *Knoppix 3.7 roCA Version 0.2.1*, disponible en Internet. (http://www.intrusion-lab.net/roca/) (21 julio 2006)
- RSA Laboratories, *RSA Security – RSA Laboratories*, disponible en Internet. (http://www.rsasecurity.com/node.asp?id=1012) (21 julio 2006)
- TinyCA, *TinyCA*, disponible en Internet. (http://tinyca.sm-zone.net/) (21 julio 2006)
- Wikipedia, *Portada: Wikipedia, la enciclopedia libre*, disponible en Internet. (http://es.wikipedia.org/wiki/Portada) (21 julio 2006).