

PRÁCTICA DE LABORATORIO Open CA

Objetivos:

El objetivo de esta práctica es mostrar al participante una utilidad práctica de una PK, es la obtención de Certificados Digitales para cifrar y/o firmar digitalmente el correo electrónico.

Esta práctica utilizará una Autoridad de Certificación de código abierto: Open CA. La misma estará corriendo desde un LiveCD con Knoppix. Mucha Suerte!!!

Nota: VERIFIQUE DE LOS SERVIDORES. LOS MISMOS PUEDEN CAMBIAR CON RESPECTO A LOS MENCIONADOS EN LA PRÁCTICA.

LAS PANTALLAS TAMBIÉN PUEDEN VARIAR DE ACUERDO AL NAVEGADOR QUE UD. UTILICE PARA LA PRÁCTICA.

Desarrollo:

PARTE 1. Solicitando un Certificado Digital.

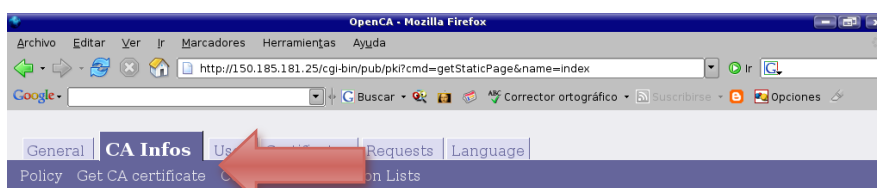
3. Diríjase a la cara pub de la RA (levante Mozilla y vea un cuadro a su izquierda) para solicitar un Certificado Digital para firma de correo electrónico. Al acceder al sitio observara la siguiente ventana.



Module	Version
OpenSSL	0.9.103
Tools	0.4.3
DB	0.9.99
Configuration	1.5.3
TRISStateCGI	1.5.5
REQ	0.9.54
X509	0.9.52
CRL	0.9.22
PKCS7	0.9.17

Terminado

4. Realice un clic en “CA Infos”



Server Information for OpenCA Server Version 0.9.2

Fri May 26 17:18:20 2006

Module	Version
OpenSSL	0.9.103
Tools	0.4.3
DB	0.9.99
Configuration	1.5.3
TRISateCGI	1.5.5
REQ	0.9.54
X509	0.9.52
CRL	0.9.22
PKCS7	0.9.17

Terminado

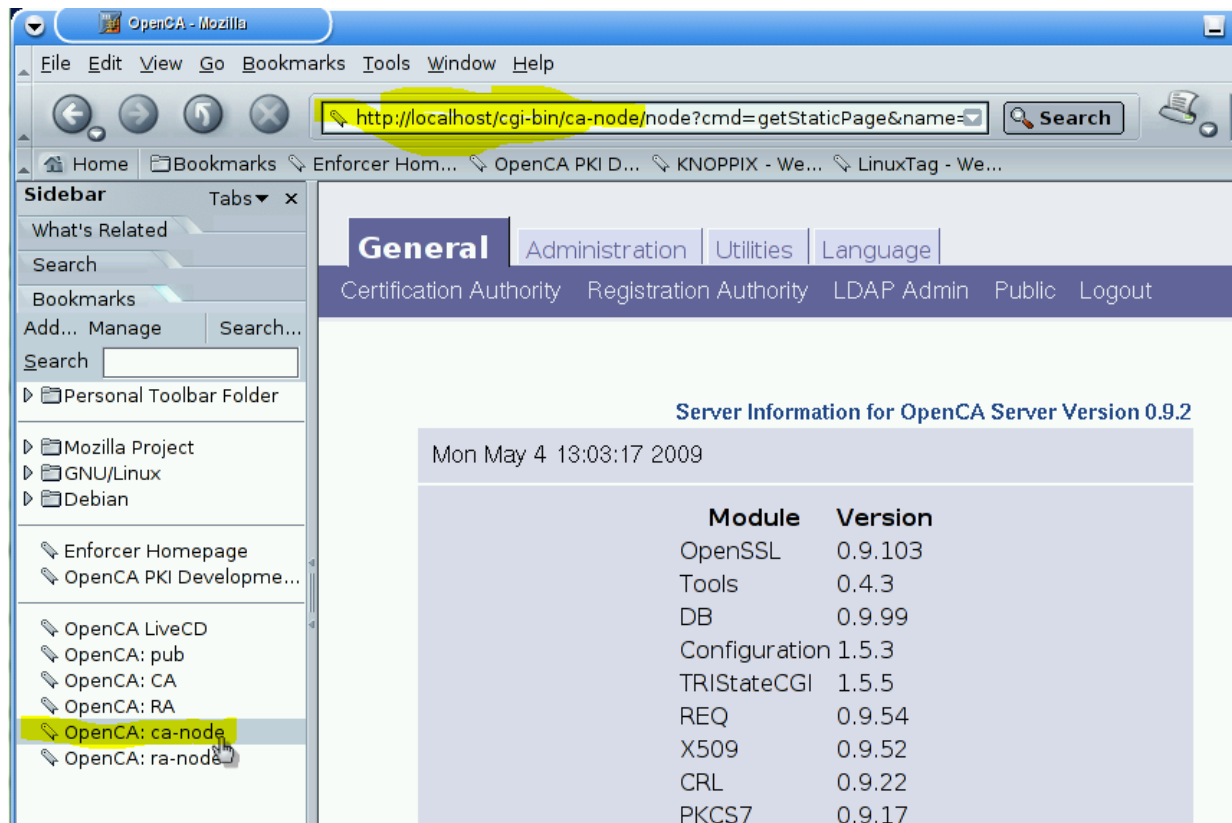
3. Instale el Certificado Raíz de la Autoridad de Certificación



4. Comente la importancia de este paso. Seleccione la opción que más se adecue al navegador que está utilizando
5. ¿Falló el paso? Comente por qué. No pase a la siguiente hoja hasta que haya llenado en el espacio que sigue por qué fallo este paso. Recuerde pensar como administrador del sistema.

Parte 2. Configurando la CA

1. PASO1: Inicializando la CA. Los pasos que seguiremos son los mismos que Ud. tendrá que seguir si desea tener operativa una PKI verdadera.



The screenshot shows a Mozilla browser window titled 'OpenCA - Mozilla'. The address bar contains the URL `http://localhost/cgi-bin/ca-node/node?cmd=getStaticPage&name=`. The sidebar on the left lists various bookmarks, with 'OpenCA: ca-node' highlighted. The main content area displays the 'General' tab of the OpenCA web interface. It includes a navigation bar with links like 'Certification Authority', 'Registration Authority', 'LDAP Admin', 'Public', and 'Logout'. Below this, a section titled 'Server Information for OpenCA Server Version 0.9.2' shows the date 'Mon May 4 13:03:17 2009' and a table of installed modules and their versions.

Module	Version
OpenSSL	0.9.103
Tools	0.4.3
DB	0.9.99
Configuration	1.5.3
TRISateCGI	1.5.5
REQ	0.9.54
X509	0.9.52
CRL	0.9.22
PKCS7	0.9.17

General

Usual Operations

Batch System

Active CSRs

Active C

Information

Language

Initialization

Configuration

Node Management

Logout

Server Information for OpenCA Server Version 0.9.

Mon May 4 13:04:47 2009

Module	Version
OpenSSL	0.9.103
Tools	0.4.3
DB	0.9.99
Configuration	1.5.3
TRISateCGI	1.5.5

General

Usual Operations

Batch System

Active CSRs

Active CR

Information

Language

Initialization

Configuration

Node Management

Logout

OpenCA Init

This page is used to initialize your PKI. Please complete carefully every phase until you continue with the next phase. All phases are required if you start initializing a new CA. If you want to recover from a crash please use the functions on the page Input and Output.

Phase I

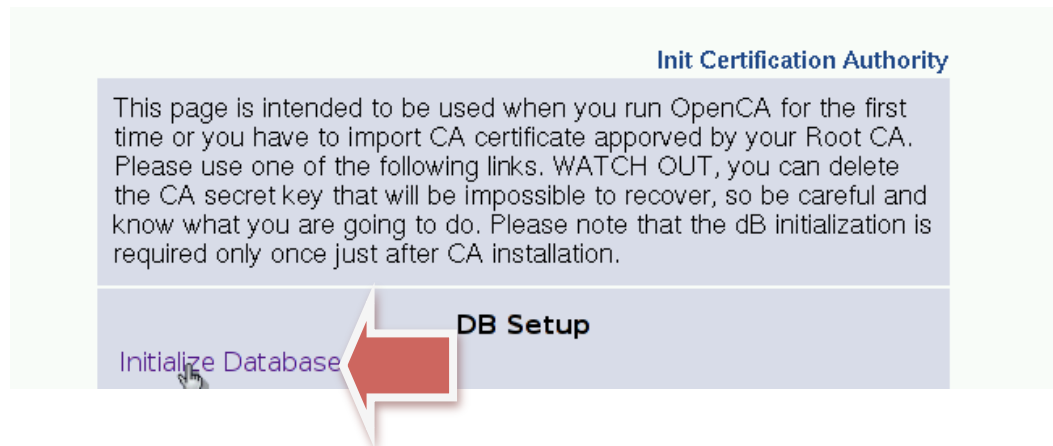
[Initialize the Certification Authority](#)

Phase II

[Create the initial administrator](#)

Phase III

[Create the initial RA certificate](#)



2. PASO 2: Hasta este punto hemos inicializado la base de datos de la CA. Ahora nos toca generar la pareja de llaves (Ku y Kp) de la CA. Recuerde que esas serán las llaves con las que se firmarán los futuros certificados.



You need to select the encryption algorithm and the CA key size (in bits).

If you are not sure, you can select the default values.

Encryption algorithm (rsa, des3, etc.)

CA key size (in bits)

Get Additional Parameters

parameters for the requested

CA secret key. Are you sure you want to generate a CA secret key?

des3

rsa

1024

OK Reset

Note la selección de los algoritmos de cifrado. A efectos de la práctica escogeremos como tamaño de la clave **1024**

Please enter your credentials.

Password

OK Reset

Este será el Password de la Clave Privada de la CA. Obviamente hay que pensar muy bien las características del mismo. POR FAVOR EN LA PRACTICA PON UNO SENCILLO Y RECUERDE

CA Secret Key Generation

Following you can find the result of the generation process.

```

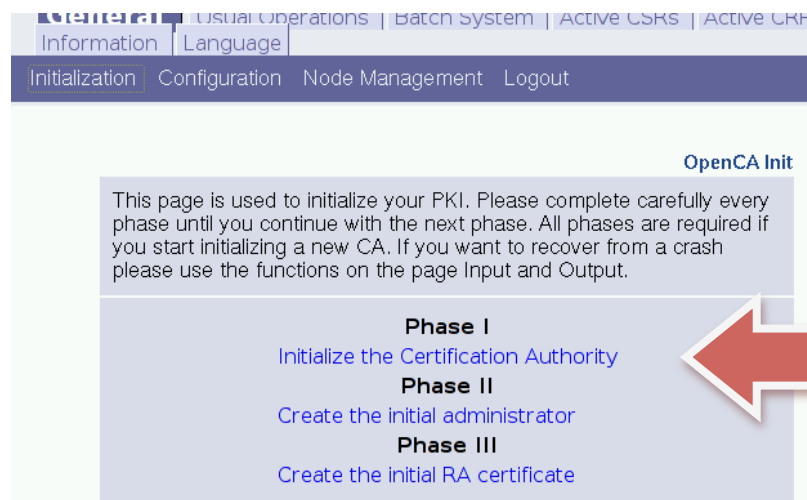
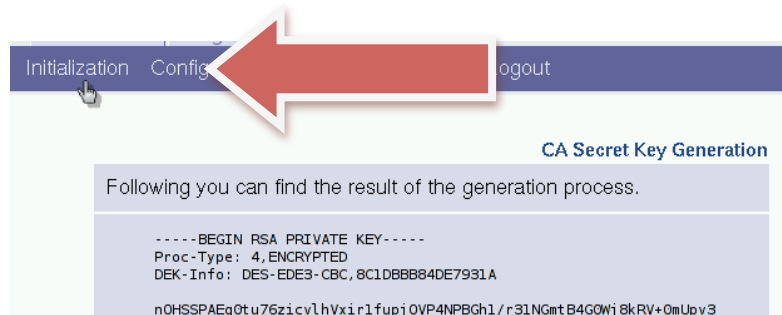
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC, 8C10BBB84DE7931A

nOHSSPAEq0tu76zicv1hVxir1fupj0VP4NPBGh1/r31NGmtB4G0Wj8kRV+0mUpv3
kIn4HeLYMM8VgqbMW4UDbPwt2ayZ7522GdrR9GfRQtVpfnWfD/WIq8wNIGhDugB
axXmofoKn1ecJLPv08xfLrt2bC7ZX1Sgpzk4m8vd1GL0/7T8JV04CvK/8i/5s5I0
zLuRBVa90gp85U1a9WPy2T2tUpPtEkxEfUWRa11unBYkM7C7MDAnnbtB00YahTi0
mEfN0o09bQuBc3zA4KBjKfWa7UCWf+miA+b7CiQseKDnbdC0vyr14G17q82YELFX
2Dn1MEr1KAzX03QdF+mMAMjg0SpeV1w6eCE9+Wd2RkNg48GF/FLLeF6C6J68PMfz
P8trG0of0u8FH0yQQJw1t9U9STQU7hiw/wOq3AJfvogyWky9XfdeP68p8Iykf9K5
ndwDC3KHh10DVyHdwUigKU/L+gRv8DdPkKLMKbjurVvKrC77zmA0Cm6iVGwSSEV
HsS4Lp8DkyL0DwZZR0qKf0yMoGIKLH6wH6Jy2LfJKJhsZB6QucYjFYuurmJbaJdM
0/M0yDRmFqKGwPODE29CMDXKK7n44zINFBGrGzVp9KwgIsthzq/WhMAiD/fu20CM
LMDq7kF2uzT4WA9LPw9oE0nmGP/NqQcicjY1FeqoNiuq4mQL79YTm4/RgxUdxef7
JA2S+VLY/UVrRYU9LnTxYlXxAgRiReJ7ShM7ipMk7wkmkjgz0Lrx61GFzZFSmTL/
qC79xkpPcL3+YymBzz/swk1sR9vFCVfSEWKR58ALLi4nLue4GxiZw==
-----END RSA PRIVATE KEY-----

```

Kp de la CA, Note que está cifrada

3. PASO 3: Ya tenemos llaves pero no Certificados. Necesitamos crear los certificados de la CA.



functionality.

Now you will be prompted with questions about the CA

certificate request. Estos datos serán de acuerdo a su CA. Póngale el nombre que desee a su empresa

simply insert. All fields can be skipped by can abort the process at any by using your browser. You must confirm the name at the end. There you can enter a distinguished name too. Are you

sure you want to continue?

E-mail address (e.g.

camanager@domain.org)

Common Name (e.g. Name

Surname)

Organizational Unit Name (e.g. MyUnit)

Organization (e.g. OpenCA)

ISO 3166 Country Code (e.g. IT, DE, US, ...)

reinaldo.mayol@localhost

Reinaldo Mayol Arnao

Universidad de Los Andes

RedULA

VE

OK

Reset

You need to enter some additional parameters for the requested functionality.

Please check the complete different the definitions of OpenSSL!

Esta es la última oportunidad para corregir algún dato.

correct or enter a butes must exactly match

emailAddress=reinaldo.mayol@localhost,CN=Reinaldo Mayol Arnao,OU=Universidad de Los Andes,C

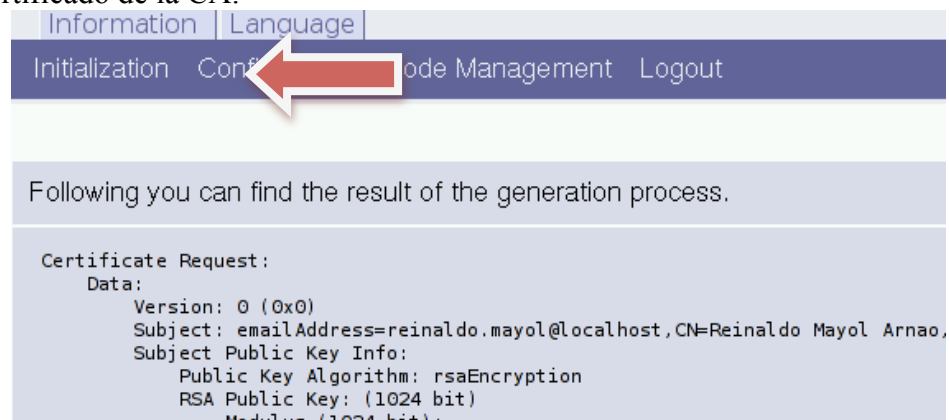
OK

Reset

Following you can find the result of the generation process.

```
Certificate Request:
Data:
  Version: 0 (0x0)
  Subject: emailAddress=reinaldo.mayol@localhost,CN=Reinaldo Mayol Arnao,OU=Universida
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        00:dc:dc:0a:29:31:2c:c5:d8:8c:f6:d8:0e:63:c2:
        40:42:53:71:3f:04:2e:c8:ad:b4:90:cb:d5:2b:9a:
        da:48:a6:5c:7c:7b:91:fd:9f:06:fa:5d:30:0c:91:
        75:d4:73:d5:dc:54:2b:aa:82:1f:a9:a3:06:c7:02:
        1f:93:1c:e1:cd:3d:d2:90:e0:1f:86:98:8e:b2:e2:
        9d:60:f1:e0:4f:02:ea:b5:e0:62:ab:23:71:34:e4:
        98:ec:11:20:37:47:89:d0:3f:2a:a6:73:3f:f6:1f:
        84:44:df:78:66:5e:64:b5:1f:41:b5:9c:34:aa:9e:
        7a:59:f5:5c:e7:b0:12:49:b5
      Exponent: 65537 (0x10001)
  Attributes:
    a0:00
  Signature Algorithm: sha1WithRSAEncryption
    da:50:c0:50:da:77:47:1c:90:06:df:2b:01:7a:07:74:61:d6:
    43:22:a3:45:fa:0c:8b:d5:43:c7:50:a0:1a:e1:63:35:60:2c:
    76:27:02:81:56:ec:aa:06:8d:9f:1e:26:19:19:e0:f3:db:33:
```

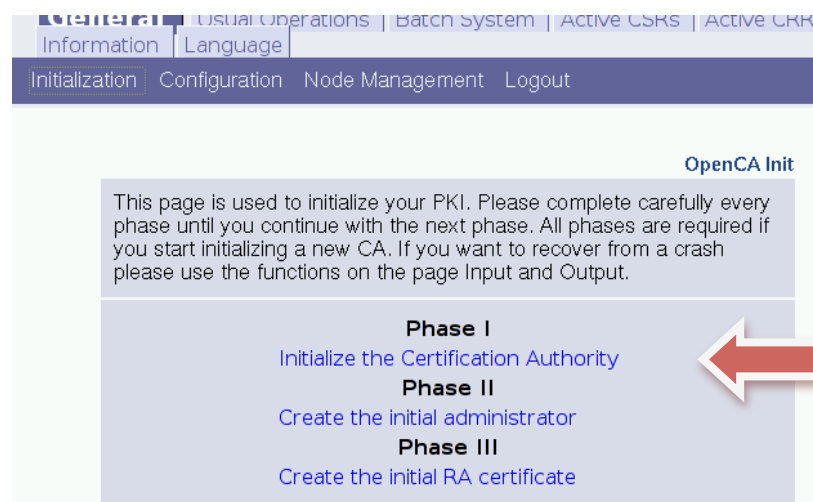

PASO 4: Hemos hecho una solicitud de certificado. En condiciones normales esta solicitud debería ser firmada por la CA de jerarquía superior que firma a la nuestra. En la práctica de hoy la firmaremos nosotros mismos. Vamos a aprobar nuestra solicitud y crear el Certificado de la CA.



Information | Language |
Initialization | **Configuration** | Node Management | Logout

Following you can find the result of the generation process.

Certificate Request:
Data:
Version: 0 (0x0)
Subject: emailAddress=reinaldo.mayol@localhost,CN=Reinaldo Mayol Arnao,
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):



General | Usual Operations | Batch System | Active CSRs | Active CSR
Information | Language |
Initialization | Configuration | Node Management | Logout

OpenCA Init

This page is used to initialize your PKI. Please complete carefully every phase until you continue with the next phase. All phases are required if you start initializing a new CA. If you want to recover from a crash please use the functions on the page Input and Output.

Phase I
[Initialize the Certification Authority](#)

Phase II
[Create the initial administrator](#)

Phase III
[Create the initial RA certificate](#)



Know what you are going to do. Please note that the DB initialization is required only once just after CA installation.

DB Setup

[Initialize Database](#)

Key pair Setup

[Generate new CA secret key](#)

Request Setup

[Generate new CA Certificate Request \(use generated secret key\)](#)

Certificate Setup

[Selfsigned CA-Certificate](#)

[Self Signed CA Certificate \(from already generated request\)](#)

[Signed by another CA](#)

[Export CA Certificate Request](#)

[Import CA certificate \(approved by Root CA \)](#)

Final Setup

[Rebuild CA Chain](#)

You need to enter some additional parameters for the requested functionality.

This option lets you create a new self signed certificate for your CA. You should have generated the private key and the CSR already. You can abort the process by using the back button of your browser. Are you sure you want continue?

CA certificate Validity (in days from now)

Following you can find the result of the generation process

Certificate:

Data:

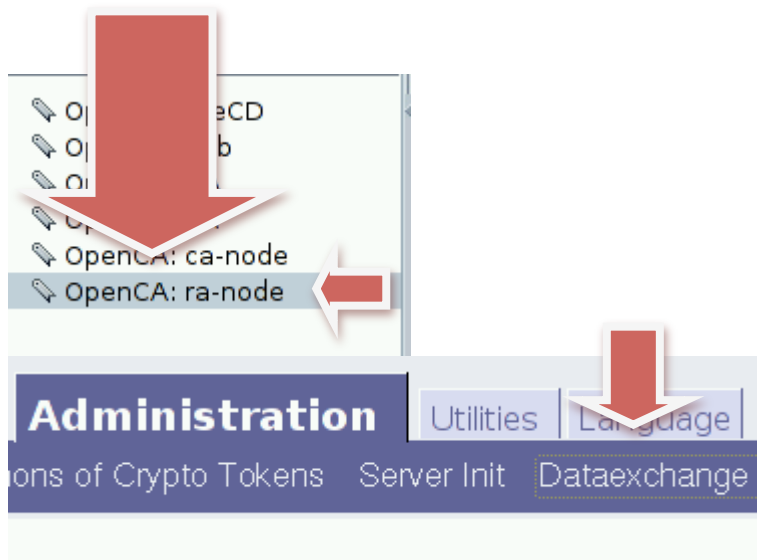
Version: 3 (0x2)
Serial Number: 0 (0x0)
Signature Algorithm: sha1WithRSAEncryption
Issuer: emailAddress=reinaldo.mayol@localhost,CN=Reinaldo Mayol Arnao,OU=Universidad de Los Andes,CO=Venezuela
Validity
Not Before: May 4 17:55:29 2009 GMT
Not After : May 4 17:55:29 2011 GMT
Subject: emailAddress=reinaldo.mayol@localhost,CN=Reinaldo Mayol Arnao,OU=Universidad de Los Andes,CO=Venezuela
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:dc:dc:0a:29:31:2c:c5:d8:8c:f6:d8:0e:63:c2:
40:42:53:71:3f:04:2e:c8:ad:b4:90:cb:d5:2b:9a:
da:48:a6:5c:7c:7b:91:fd:9f:06:fa:5d:30:0c:91:
75:d4:73:d5:dc:54:2b:aa:82:1f:a9:a3:06:c7:02:
1f:93:1c:e1:cd:3d:d2:90:e0:1f:86:98:8e:b2:e2:
9d:60:f1:e0:4f:02:ea:b5:e0:62:ab:23:71:34:e4:
98:ec:11:20:37:47:89:d0:3f:2a:a6:73:3f:f6:1f:
84:44:df:78:66:5e:64:b5:1f:41:b5:9c:34:aa:9e:
7a:59:f5:5c:e7:b0:12:49:b5
Exponent: 65537 (0x10001)

Finalmente tenemos el certificado de la CA. Ánimo casi llegamos a la mitad

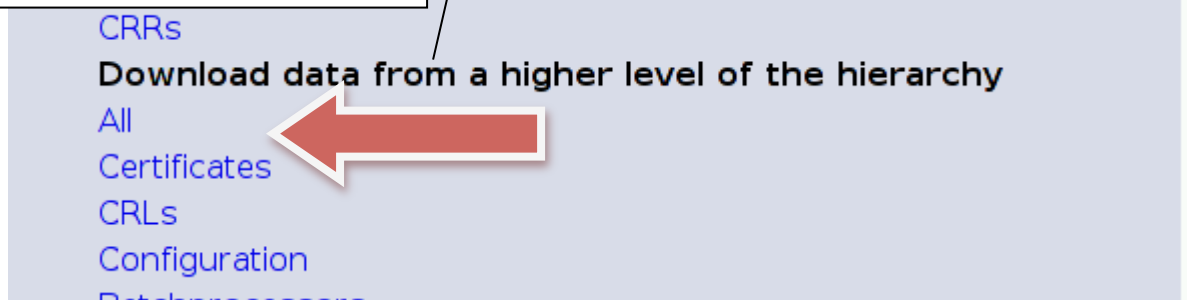
4. PASO 5: Ya tenemos Certificado Digital de la CA, ahora deberemos exportarla para que todos puedan obtenerlo. Para esto SECUENCIALMENTE realice los últimos 2 pasos de la sección **FINAL SETUP**.



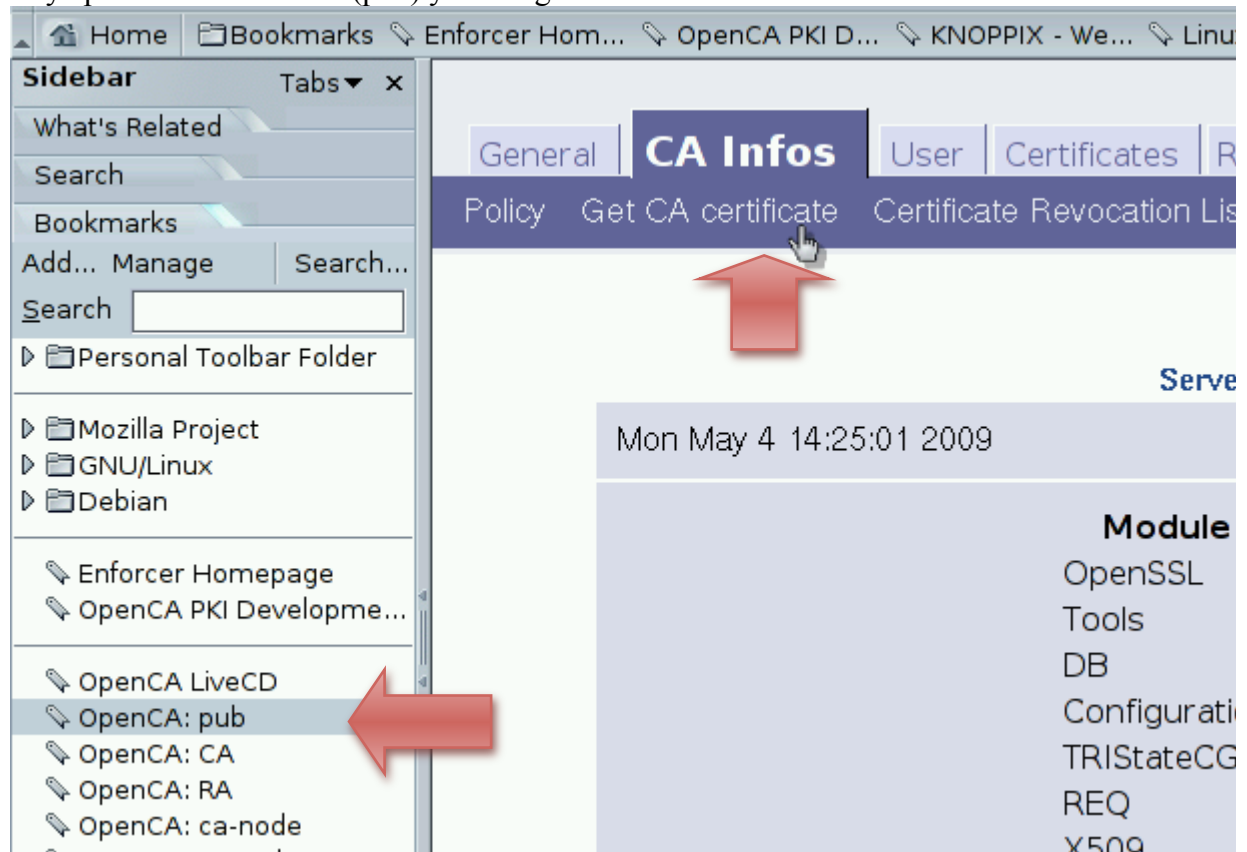
5. PASO 6. Con el último paso hemos exportado desde la CA el Certificado de la misma. Pero recuerde que los usuarios no tienen acceso a la CA sino a la RA, por lo tanto tenemos que importar en la RA el Certificado creado. Este paso es sumamente delicado y en condiciones normales debe hacerse con sumo cuidado. ¿Imagina que sucedería si el Certificado de la CA es adulterado? Vamos a exportar el certificado.

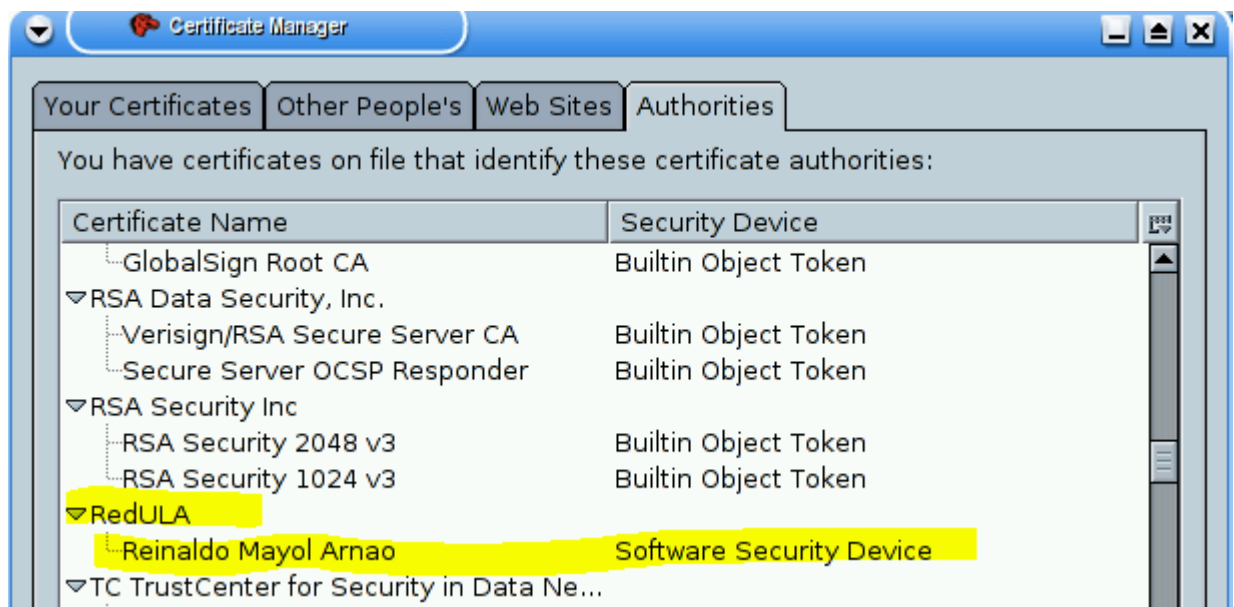


Note que esta descargando desde un nivel superior (CA->RA)



6.1 Ahora ya podremos ir a la RA (pub) y descargar el certificado de la CA.





Note que hemos creado una CA que lleva nuestro nombre. Lo hemos hecho así a efectos de la sencillez de la práctica, pero en condiciones reales esto no sería una buena idea. **RECUERDE ESTE ES UN CERTIFICADO DE AUTORIDAD DE CERTIFICACION!!!!!!**

6. PASO 7. Ya tenemos la CA lista pero no tenemos Operador para la CA, es decir no tenemos quien la opere. Debemos repetir todo el proceso pero ahora para el Operador de la CA. Volvamos a la CA y a la ventana de Inicialización.



This page is intended to be used when you run OpenCA for the first time. Please use the following links to create the first user of the PKI. This user should be an administrator.

Init first user workflow

[Create a new request](#)

[Edit the request](#)

[Issue the certificate](#)

[Handle the certificate](#)



Certificate Data

E-Mail	rootCA@localhost
Name	Operador CA
Certificate Request Type	Internet
Name (first and last name)	Operador CA
Email	rootCA@localhost
Department	Seguridad Informatica
Telephone	5555555
Level Of Assurance chose the LOA you would like to be authenticated against.	High
Role	CA Operator
Registration Authority chose the RA where you will be authenticated	Trustcenter itself
PIN [used to verify the request, min 10 chars (please verify after usage)]	512
Re-type your PIN for confirmation	512
Choose a keysize	512

Continue

Recuerde que son los datos del Operador CA

512 ; Recuerde que está corriendo en request, min 10 chars (please verify after usage)]

Listo! Hemos hecho la SOLICITUD de Certificado del Operador CA. Ahora nos queda aprobar la solicitud y emitir el certificado.

General Usual Operation

Language

Initialization



This page is intended to be used when you run OpenCA for the first time. Please use the following links to create the first user of the PKI. This user should be an administrator.

Init first user workflow

[Create a new request](#)

[Edit the request](#)

[Issue the certificate](#)

[Handle the certificate](#)



Used

Identification 01b307acba4f54f55aafc33bb06bbbf6ca803e9a

PIN

Modulus
(key size) 512

Public Key
Algorithm rsaEncryption

Signature
Algorithm sha1WithRSAEncryption

Name (first
and Last
name)

Operador CA

Email

rootCA@localhost

Department

Seguridad Informatica

Telephone

5555555

RA

Trustcenter itself



Submit the changed request

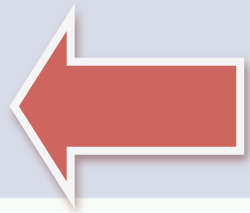
Cancel the changes

Operations

Edit the request

Issue certificate

Delete request



LISTO ;!! Tenemos el Certificado del Operador CA! Mire los detalles

Certificate Issued

Description Certificate issued and Certificate Request archived.

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 1 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: emailAddress=reinaldo.mayol@localhost,CN=Reinaldo Mayol Arnao,OU=Universidad
  Validity
    Not Before: May  4 18:57:52 2009 GMT
    Not After : May  4 18:57:52 2010 GMT
  Subject: serialNumber=1,CN=Operador CA,OU=Internet,O=OpenCA LiveCD Demo CA,C=US
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (512 bit)
      Modulus (512 bit):
        00:bc:30:9a:9d:46:85:d9:ec:e1:9a:89:0e:4e:b7:
        28:c2:2b:26:e6:bb:8e:a1:ee:fb:ab:3e:14:77:cc:
        29:18:86:14:b9:ba:86:04:d2:63:7b:10:ad:40:33:
        c4:1a:89:5d:ec:3a:7a:1f:0f:95:96:70:38:30:04:
        7e:ea:43:8e:9d
      Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Basic Constraints:
```

Finalmente instalemos el certificado en el navegador y hemos concluido el proceso de Instalación de la CA. (Realmente tendríamos que hacer algo parecido en la RA (o las RA si hay varias, pero a efectos de la práctica lo dejaremos hasta aquí.)

This page is intended to be used when you run OpenCA for the first time. Please use the following links to create the first user of the PKI. This user should be an administrator.

Init first user workflow

[Create a new request](#)

[Edit the request](#)

[Issue the certificate](#)

[Handle the certificate](#)



Operations

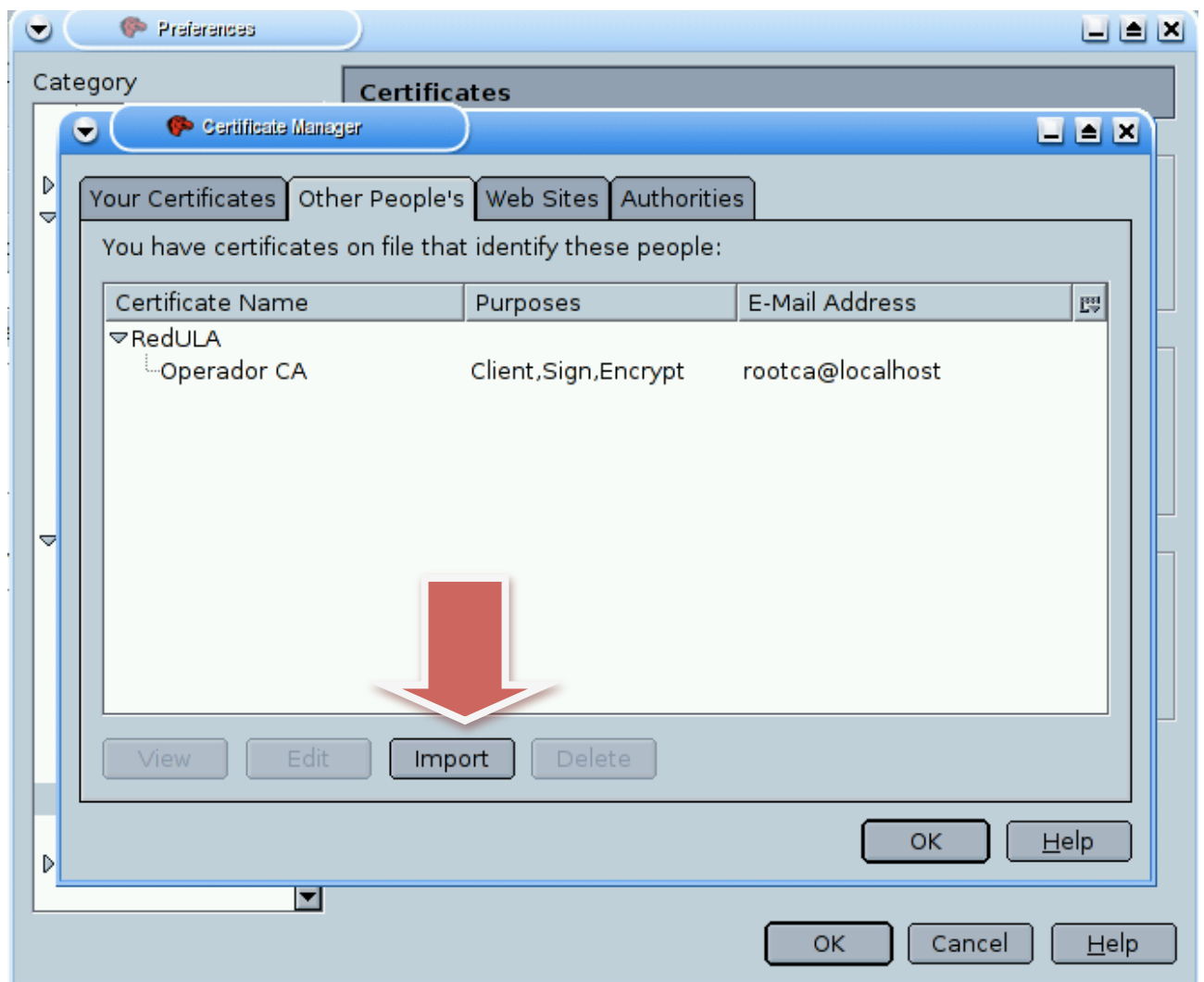
CSR's Serial Number	256
Certificate	PEM ▾ Download
Certificate and Keypair	SSLLeay (mod_ssl) ▾ Download
Change Passphrase	Change
Remove Key from database	Remove
Tokenhandling	Download certificate onto token
Set passphrase for key enrollment	Set passphrase

Descargue el Certificado Y LA
CLAVE PRIVADA!!

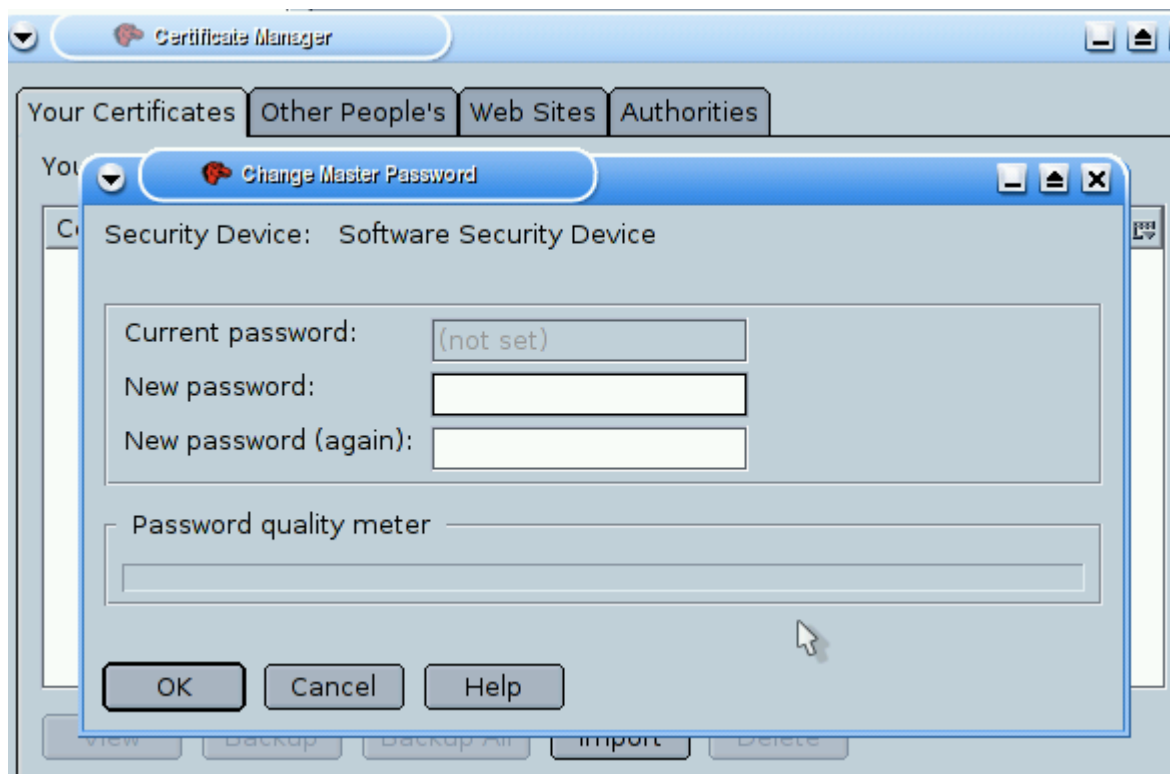
Operati

CSR's Serial Number
Certificate
Certificate and Keypair
Change Passphrase
Remove Key from database
Tokenhandling
Set passphrase for key enrollme

Salve el certificado creado. De inmediato pasaremos a instalarlo en nuestro navegador y listo. Ya estamos listos para comenzar a trabajar con la CA. Recuerde que debe hacerlo desde las preferencias de su navegador. En la imagen (ya que es una prueba) se muestra como un certificado ajeno. Sin embargo, en su caso DEBE ser propio (Your Certificates)



Ahora tendrá que ponerle password a su “ Software Security Device”



Podemos ver las características del certificado instalado.

