MANUAL DEL USUARIO

MANUAL DEL ADMINISTRADOR DE LA AUTORIDAD CERTIFICADORA

MANUAL DEL ADMINISTRADOR DE LA AUTORIDAD REGISTRADORA

INDICE

1 CA INITIALIZATION 6
1.1 Phase I: Initialize the Certification Authority 6
1.1.1 Database Setup 6
1.1.2 Key pair setup 6
1.1.3 Request setup 6
1.1.4 Certificate setup 7
1.1.5 Selfsigned CA certificate 7
1.1.6 Signed by another CA 7
1.1.7 IFinal setup 7
1.2 Phase II and III: Create the initial administrator and RA certificate 8
2 CSR Handling - a request HOWTO 8
2.1 Ways to request a certificate 9
2.2 Edit a certificate signing requests 10
2.3 Approve certificate signing requests 10
2.4 Delete certificate signing requests 10
3 CERTIFICATE HANDLING 10
3.1 Find a certificate 10
3.2 Download 11
3.2.1 Direct Download 11
3.2.2 Downloads from certificate page 11
3.2.2.1 Normal Downloads 11
3.2.2.2 Private Key Downloads 12
3.2.2.3 Certificate Installation 12
3.3 Star Revocation 13
3.4 Write an email to the owner 13
3.5 Informations and their meaning 13
4 PUBLIC PKI SERVER 14
4.1 CA 14
4.1.1 Get CA Certificate 14
4.1.2 Certificate Revocation Lists 15
4.2 User 15
4.2.1 Request a certificate 16
4.2.1.1 Request a certificate with automatic browser detection. 17
4.2.1.2 Basic Request 17
4.2.1.3 Netscape´s Request 17
4.2.1.4 IE Request 17
4.2.1.5 Server Request 17

4.2.1.6 Token Request 18
4.2.2 Get Requested Certificate 18
4.2.3 Test Certificate 18
4.2.4 Revoke Certificate 19
4.3 Certificates 19
4.3.1 Valid 19
4.3.2 Expired 20
4.3.3 Revoked 20
4.3.4 Suspended 20
4.3.5 Search 21
4.4 Requests 21
4.4.1 Certificate Requests List 21
4.4.2 Certificate Revocation Requests List 21
5 AUTORIDAD REGISTRADORA 22
5.1 Administration 22
5.1.1 Server Management 22
5.1.2 LDAP Admin 22
5.2 Pending Request 23
5.2.1 Certificate Request 23
5.2.1.1 Edit Request 23
5.2.1.2 Approve an Sign Request 23
5.2.1.3 Approve Request without Signing 24
5.2.1.4 Delete Request 24
5.2.2 Revocation Requests 24
5.3 Information 24
6 REGISTRATION AUTHORITY NODE 25
6.1 Gateways 25
6.1.1 Certificate Authority 25
6.1.2 Registration Authority 25
6.1.3 LDAP 25
6.1.4 Public 26
6.2 Administration 26
6.2.1 Server INIT 26
6.2.1.1 Initialise DataBase 26
6.2.1.2 Impot Configuration 26
6.2.2 Dataexchange 26
6.2.2.1 Enroll data to a lower lever of the hierarchy 27
6.2.2.2 Receive Data form a lower level the hierarchy 27

6.2.2.3 Download Data from a higher level the hierarchy 27
6.2.2.4 Upload data to higher level of the hierarchy 28
6.2.3 Backup and Recovery 29
6.2.3.1 BackUp DataBase 29
6.2.3.2 Recovery Initialize DataBase 29
6.2.3.3 OpenCA …. DB-DB if you use DBM-files 29
6.2.3.4 OpenCA …. DB-DB if you use a SQL – database 29
6.2.3.5 Rebuild OpenSSL's database and next serial number 29
6.2.4 Database Handling 30
6.3 Utilities 30
6.3.1 E-Mail New Users 30
6.3.2 Send a CRIN-mail 30
6.3.3 Delete Temp Files 30
7 LDAP INTERFACE 30
7.1 Update LDAP 31
7.1.1 CA-Certificate 31
7.1.2 Certificates 31
7.1.3 CRL 31
7.2 View CA-Certificates 31
7.2.1 Valid 31
7.2.1.1 Add to LDAP 31
7.2.1.2 Add to LDAP with modified DN 32
7.2.1.3 Delete from LDAP 32
7.2.1.4 Delete from LDAP with modified DN 32
7.2.2 Certificates Expired 32
7.3 View Certificates 32
7.3.1 Valid 32
7.3.1.1 Add to LDAP 32
7.3.1.2 Add to LDAP with modified DN 32
7.3.1.3 Delete from LDAP 33
7.3.1.4 Delete from LDAP with modified DN 33
7.3.2 Expired 33
7.3.2.1 Add to LDAP 33
7.3.2.2 Add to LDAP with modified DN 33
7.3.2.3 Delete from LDAP 33
7.3.2.4 Delete from LDAP with modified DN 33
7.3.3 Suspended 34
7.3.3.1 Add to LDAP 34

7.3.3.2 Add to LDAP with modified DN 34
7.3.3.3 Delete from LDAP 34
7.3.3.4 Delete from LDAP with modified DN 34
7.3.4 Revoked 34
7.3.4.1 Add to LDAP 35
7.3.4.2 Add to LDAP with modified DN 35
7.3.4.3 Delete from LDAP 35
7.3.4.4 Delete from LDAP with modified DN 35
7.4 View CRLs 35
7.4.1 CRLs 35
7.4.1.1 Add to LDAP 35
7.4.1.2 Add to LDAP with modified DN 36

MANUAL DEL ADMINISTRADOR DE LA CA

1 CA INITIALIZATION

La inicialización de la CA consiste de tres fases y puede ser ejecutada una sola vez. La primera fase es obligatoria. Esta se inicializa a si misma. La segunda y tercera fase son opcionales, donde se crean los primeros dos certificados. La fase dos crea el primer certificado para un operador y la fase tres se crea un certificado para el servidor web en línea.

1.1 Phase I: Initialize the Certification Authority

La primera fase de la inicialización del OpenCA es usado para iniciar todos los mecanismos de criptografía que son necesarios para ejecutar la CA. Esta incluye cosas como crear la llave privada, un Certificate Signing Request (CSR), un certificado para la CA y las cadenas de la CA. Si usted completara esta fase con éxito entonces la CA esta lista para su uso operacional. Las otras fases sólo hacen algunas tareas optativas.

1.1.1 Database Setup

El Database Setup inicializa la base de datos. Si se usa OpenCA::DB entonces el backend consiste en archivos DBM. Si se usa OpenCA::DBI entonces el backend consiste de una base de datos SQL. Para nuestro propósito se utilizará MySQL aunque pueden ser usadas también PostgreSQL, IBM DB2 y Oracle.

1.1.2 Key pair setup

Aquí se realiza la generación de la llave privada para la CA. El algoritmo de la llave se genera así misma, el algoritmo de cifrado de la llave y la longitud de la llave. Al dar entrada a todos los parámetros criptográficos entonces hay que escribir el password de la fase (passphrase).

1.1.3 Request setup

Si usted necesita crear una nueva solicitud de certificado, entonces para crear el certificado de la CA usted tendrá que llenar cierta información que se necesita para crear un certificado del estilo "emailAddress =... ,cn =... ,ou =... ,o =... ,c =...". Después de que usted introdujo todos los datos, OpenCA desplegará el asunto completo de la solicitud. Ésta es la última oportunidad que tendrá para modificar el asunto.

1.1.4 Certificate setup

Hay dos opciones generales para un certificado de CA en OpenCA. Usted puede usar el CA como una raíz se tiene que crear un certificado que sea auto firmado o utilizar otra CA y dejarlo firmar su solicitud de certificado.

1.1.5 Selfsigned CA certificate

Si se desea crear un nuevo root CA entonces simplemente se crea un nuevo certificado para la CA auto firmado. Esto es mucho mas simple que inicializar o crear una nueva sub Autoridad Certificadora pero puede ser más peligroso.

1.1.6 Signed by another CA

Primero se tiene que exportar la solicitud a la root CA que tiene que emitir el certificado de la CA. OpenCA crea un archivo tar para la exportación. Este archivo tar contiene careq.pem. Este archivo es la solicitud en formato PKCS#10. La descodificación es un PEM (base64). Es necesario ir a la raíz de la CA y seguir las instrucciónes para el proceso de la solicitud.

Si la root CA emite un certificado para una nueva sub CA entonces se tiene que crear un archivo tar para su importación. El archivo tar contiene el archivo cacert.pem que es el nuevo certificado de la CA. Al dar click en el link para la importación del nuevo certificado de la CA entonces OpenCA copia los archivos a todos los lugares necesarios.

1.1.7 IFinal setup

Los últimos pasos también pueden hacerse adelante en la de la node management pero es una buena idea hacerlo durante la inicialización y conseguir un estado consistente. La reconstrucción de las cadenas de CA son necesarias para verificar la correcta firma digital. Si se desea una sub CA entonces se debe de agregar todos los certificados de la autoridad Certificadora en in PEM format en el directorio OPENCADIR/var/crypto/chain/ antes de reconstruir la cadena.

El ultimo paso es exportar la configuración dentro del servidor en línea. Los demás usuarios ignoran este paso y maneja la comunicación entre los diferentes nodos de la PKI vía interfase de los nodos de administración. Si esta es la primera vez que se usa OpenCA entonces se debe de exportar la configuración e importar dentro del servidor.

1.2 Phase II and III: Create the initial administrator and RA certificate

Estas dos fases son usadas para crear los primeros certificados de la infraestructura. Se pueden crear estos certificados por medio de una RA e interfase publica pero también, normalmente las personas pueda que quieran hacerlo en línea desde la RA y corriendo https. Para que ellos puedan realizarlo se necesita como mínimo un certificado para el servidor de tejido de RA. Si ellos usan un online RA debe ser entonces una solución segura que los operadores deben firmar una solicitud, si ellos aprueban una solicitud. Para que ellos puedan tener un certificado de usuario inicial. Si los operadores tienen al login vía una firma digital y no con login y passphrase entonces el primer certificado del usuario es obligatorio. Si usted compara los dos screenshots entonces se podrá ver que sólo los nombres de las formas difieren. Ambas fases usan el mismo proceso para cada certificado normal que se firma para la solicitud. Solo pueden leer la sección de guía del usuario donde se describe las diferentes solicitudes y su manejo.

Las fases consisten en cuatro pasos:

- **Crear una Nueva Solicitud**
- **Revisar la Solicitud**
- **Emitir el Certificado**

2 CSR Handling - a request HOWTO

Normalmente un administrador o un usuario necesita más seguridad, de repente se asusta del alto riesgo que existe si el quiere solicitar un certificado. Éste es el momento en el que se debe estar listo parra presentar una pequeña explicación de cómo es el proceso de certificación. Se ha dividido en cinco más dos partes:

1. cómo realizar la nueva solicitud
2. cómo revisar una solicitud
3. cómo aprobar una solicitud
4. cómo emitir un certificado
5. cómo enrollarse un certificado
6. cómo anular una solicitud
7. las explicaciones de los campos de la entrada

Hay un segundo tipo de solicitud: la solicitud de revocación de certificado (CSR).

2.1 Ways to request a certificate

Los certificados X.509 son muy bien conocidos y el formato realmente se establece pero en los primeros años existieron algunos problemas con las solicitudes porque no había ningún protocolo simple para realizar solicitudes vía interfase del cliente. El resultado es que se regularizó un formato para las solicitudes y un formato para el propietario.

El formato de la solicitud normal es PKCS#10 qué es apoyado por todos los servidores (tejido del ej., mande por correo, VPN) y Microsoft Internet Explorador. Netscape desarrolló un propio formato llamado SPKAC. Este formato de propiedad se usa hoy por Mozilla y Ópera.

Hay software sorprendentemente disponible qué acostumbra emitir o aplicar certificados y las llaves privadas, a los datos del encrypt como emails o https-conexión pero no pueden crear una llave privada o una solicitud. De este tipo de software es el konqueror de KDE en estos dias. Este software simplemente carga una llave privada ya emitida y un certificado.

La Solicitud es sólo para datos pero nosotros lo necesitamos también como un procedimiento para la creación y transporte de la solicitud. Los browsers están de dos maneras

- Microsofts CAPI (Microsoft Internet Explorador) y la etiqueta de Netscape "keygen" (Mozilla, Netscape, la Ópera). Una tercera manera es la manera de konqueror que espera que nosotros hagamos todo por él.

Una segunda área es la de servidores. A algunos servidores les gusta que el apache tenga el mismo funcionamiento que el konqueror. Para que le realicen la generación de las llaves y sea manejable o ir a la interfase pública de PKI y permitir que la PKI haga el trabajo. A algunos otros servidores les gusta que el servidor de VPN pueda generar llaves privadas y solicitudes por sí mismo. Los servidores y clientes de VPN apoyan en contraste con el web browsers dos protocolos de transporte - la manera manual y SCEP. Normalmente se puede copiar la solicitud a un disco blando y puede ir a su PKI o si usted acostumbra a SCEP para manejar toda la comunicación automáticamente con la PKI.

2.2 Edit a certificate signing requests

Si un usuario introduce una solicitud entonces esta solicitud debe ser verificada por un operador. El operador puede mirar la solicitud usando la lista de solicitudes o investiga en el banco de datos.

2.3 Approve certificate signing requests

Si un operador de RA está seguro que todo las informaciones son ahora entonces correctas él puede aprobar la solicitud. Usted puede hacer esto con y sin una firma digital. La firma digital afianza la demanda contra la manipulación después de la aprobación.

2.4 Delete certificate signing requests

Usted tiene la opción para anular una Solicitud. Esto es necesario si una solicitud tiene que ser rechazada por una PKI.

3 CERTIFICATE HANDLING

Esta sección describe todas las cosas que puede hacer con un certificado desplegado.

3.1 Find a certificate

Usted puede encontrar un certificado con dos métodos. El primer método es la búsqueda. Vaya a Utilities → Sarch certificate. Puede entrar algunos parámetros en la forma de búsqueda desplegada. El formulario únicamente acepta comodines si usa una base de datos SQL. Si la búsqueda es exitosa entonces puede escoger el certificado que será desplegado.

El segundo método es un poquito mas tonto. Vaya a Certificates → Valid y trate de encontrar el certificado apropiado en la lista. Puede navegar usando los links en línea Extra Referentes.

3.2 Download

3.2.1 Direct Download

Puede descargar directamente un certificado en su buscador ingresando una serie apropiada. Tiene que saber la serie del certificado, de la solicitud de su ID en el proceso serial. El buscador será detectado automáticamente por el software. Por favor recuerde que este método únicamente trabaja si genero la llave privada con este buscador y la llave privada esta todavía en el almacenador de llaves en su computadora.

3.2.2 Downloads from certificate page

Hay tres formas diferentes de descargar un certificado. Puede descargar datos pasivos. Puede descargar la llave privada y el certificado y puede instalar el certificado de otro usuario. Si usted ya tiene la llave privada y desea instalar un nuevo certificado en su buscado entonces por favor use la descarga directa porque es la única parte del software que envía paginas especiales HTML para la instalación de certificados directos.

3.2.2.1 Normal Downloads

Si usted únicamente necesita un certificado en un formato especial entonces puede elegir el formato y dar clic en Download. El certificado será enviado con un tipo MIME apropiado el cual previne la instalación de buscadores. Usted puede salvar el certificado en un disco y puede hacer lo que desee hacer con el.

3.2.2.2 Private Key Downloads

Si quiere descargar un certificado y la llave privada hay dos posibilidades. Si la operación es permitida en su interfase y el switch de configuración REQUIRE_PASSWD_PUBLIC en puesto en no entonces puede dar clic en descargar. Si necesita la llave en un formato diferente del PKCS#8 entonces tiene que ingresar la clave para convertir la llave privada. Después de esto recibirá la llave y el cerificado y puede salvarlos.

Si la operación es permitida en su interfase y el switch de configuración REQUIRE_PASSWD_PUBLIC esta puesto en si entonces tiene que irse a su operador RA y pedirle que ponga la clave. Hacemos esto para evitar ataques de denegación de servicio en contra de la clave privada de un usuario. Es altamente recomendado borrar la clave después de un periodo corto de tiempo y generar las claves con cosas como openssl rand. Las claves generadas por los usuarios o administradores no son muy seguras. Si el administrador pone la clave para este certificado vía la interfase RA entonces puede ir nuevamente a su interfase y descargar el certificado y la llave privada. Tiene que ingresar la clave para la llave privada primero y luego el software le pregunta por una segunda clave para otorgar su acceso al comando de exportación. Si descargo la llave entonces por favor informe al Operador RA y solicítele que remueva la clave para evitar ataques de denegación de servicio en contra de su clave privada.

3.2.2.3 Certificate Installation

Algunas veces usted necesita un certificado de otro usuario que nunca envía un correo firmado. Si tiene una instalación normal con soporte LDAP entonces puede buscar el certificado en el directorio. Hay instalaciones donde este servicio no esta disponible. En este caso puede ir a la pagina de certificados y si esta activada la función apropiada en la configuración entonces puede dar clic en instalar y el certificado será automáticamente instalado en su almacenador de certificados. Después de esto puede usarlo para cifrar emails.

3.3 Star Revocation

3.4 Write an email to the owner

3.5 Informations and their meaning

4 PUBLIC PKI SERVER

Esta sección describe la interfase pública para el OpenCA PKI. Desde estas pantallas un usuario puede ver la lista de certificados actuales, certificados de administración y descarga CA y los certificados de revocación.

4.1 CA

Esta sección describe las utilidades CA relacionadas a las que el usuario puede acceder. Cada encabezado abajo relaciona a un link en la barra de menú del lado izquierdo.

4.1.1 Get CA Certificate

Entrando a este link el usuario se encuentra con una página titulada “CA-Certificate Page”. Esta página contiene links a certificados CA en varios formatos.

Con el propósito de que el usuario “confíe” en los certificados generados por medio de OpenCA, éstos tienen que tener instalado el certificado raíz Certificado de Autoridad. Esta página les provee un mecanismo sencillo de hacerlo. La mayoría de usuarios solamente darán un clic en “CA-cetificate in format CRT” y seguirán las instrucciones presentadas por el ambiente (e.g. En IE ellos tienen la opción de “Abrir” el archivo y luego “instalar el Certificado”).

Los administradores del servidor Apache Web podrían usar el link “CA-certificate” para descargar el certificado en el formato apropiado para incluirlo en los archivos de configuración Apache.

4.1.2 Certificate Revocation Lists

Entrando a este link el usurario se encuentra con una pantalla titulada “CRL Page”. Esta página contiene links a listas de certificados de revocación en varios formatos.

Muchos clientes de certificados (como Microsoft Outlook y Netscape Navigator) hacen uso de listas de certificados de revocación para asegurarse que los certificados son aún válidos y no han sido revocados.

Tres links son proporcionados, cada uno conteniendo el CRL en un formato diferente, dependiendo del cliente. El cliente normal podrá descargar el CRL en formato DER para incluirlo en sus buscadores. Los administradores de servidores web podrán usar el formato PEM. El formato de texto es descargado como un file humanamente leíble.

4.2 User

Esta sección permite al usuario manejar sus certificados. Permite solicitar certificados, prueba y revocación.

4.2.1 Request a certificate

Este link presenta al usuario una página ofreciendo varios métodos de solicitar un certificado. Hay diferencias sutiles entre los métodos, las cuales son descritas abajo. Cada uno de los links llevará al usuario a un formulario. El usuario llenará el formulario y someterá los datos. Los datos sometidos serán usados para crear la firma de certificado solicitada (CSR) la cual irá la al Autoridad de certificado para ser firmada y regresará como un certificado.

El formulario de datos tiene los siguientes campos:

- E-Mail: La dirección de correo electrónico asociada con el certificado.
- Name: Nombre del usuario.
- Certificate Request Group: Este es usualmente el departamento o sub grupo al cual el usuario pertenece.
- Role: La función del certificado entre la jerarquía, esto es usualmente “usuario” para la mayora de los usuarios normales.
- Registration Authority: Esto es usualmente la localización física en la cual el usuario será identificado (e.g. personal)
- PIN: una clave usada para verificar el CSR
- Key Size: El tamaño de la clave usada en el CSR (usualmente basada a 1024

Después de completar el formulario el siguiente grupo de pantallas que el usuario ve dependerá del cliente que se está utilizando y el tipo de solicitud seleccionada. Después de que el CSR ha sido generado y sometido al usuario le será emitido un Certificate Request ID (identificación de solicitud de certificado). Este toma la forma de un número integer. Es importante que el usuario anote este número porque será requerido cuando recupere su certificado.

Una vez que el usuario ha solicitado su Certificado de Autoridad procesará la solicitud de certificado. Esto puede envolver una identificación cara a cara del usuario y el Trust Center. Cuando el certificado ha sido creado el usuario será informado por email. Este email incluirá también el Número de Revocación de Certificado (CRIN), este número debe conservarse en un lugar seguro pues será requerido si el usuario necesita revocar su propio certificado en el futuro.

4.2.1.1 Request a certificate with automatic browser detection.

Presionando este link, OpenCA tratará de determinar qué buscador está utilizando el usuario para solicitar su certificado. Una vez que esto ha sido establecido, el formulario CSR es presentado al usuario. El CSR (con las llaves públicas y privadas asociadas) será generado por el buscador del usuario y sometido al Certificado de Autoridad.

4.2.1.2 Basic Request

Este link guía a una clave de servidor y a la generación de CSR. El usuario podrá usar este link si su buscador no apoyó la generación de CSR, o si por alguna razón ellos querían que el Certificado de Autoridad generara las claves y CSR (e.g. Para copia de seguridad de la clave en el servidor).

4.2.1.3 Netscape´s Request

Este link debe ser utilizado si el cliente es un buscador del tipo Netscape (e.g. Navigator o Mozzilla). El CSR generado por el cliente será del tipo SPKAC.

4.2.1.4 IE Request

Este link deberá ser usado si el cliente es un buscador el tipo Internet Explorer. El CSR será generado por el cliente.

4.2.1.5 Server Request

Este Link es usado para someter una solicitud de certificado de servidor web. Este es ligeramente diferente de la solicitud de un cliente normal ya que el CSR habrá sido generado en el servidor web. Este es un campo utilizado para subir archivos de CSR, por lo que el usuario debe asegurarse que tiene un CSR para subir antes de seleccionar esta opción.

4.2.1.6 Token Request

Este link es el mismo que el “Basic Request” en el que las llaves y CSR son generadas en el servidor. Esta solicitud es utilizada cuando el Certificado de Autoridad va a crear la llave par y certificado en un token de hadware.

4.2.2 Get Requested Certificate

Este link provee el mecanismo para que el usuario recupere el certificado solicitado y lo instale en el buscador.

Al usuario se le presenta una pantalla y una serie de instrucciones. Lo más importante es que el usuario tiene que estar usando la misma computadora que fue usada para solicitar el certificado. Esto es importante porque ambos buscadores el tipo IE y el Netscape necesitan enlazar el certificado de regreso al CSR y llaves privadas, esto sólo puede ser hecho si la computadora que fue usada para generar el CSR es usada para recuperar el certificado.

El usuario deberá ingresar su “Número de Serie” en el espacio proporcionado. El número de serie puede ser:

Certificate´s Serial	el número serial del certificado firmado por el Certificado de Autoridad.
Request´s Serial	el número serial de la solicitud sometida, emitido por el usuario en el momento de sumisión en el CSR.
Your ID:	Es el ID el cual utilicé para el proceso secuencial. Usualmente este ID es una cuenta pero el ID fue definido por el administrador del proceso secuencial.

Presionando el botón de “Continuar”, OpenCa intenta instalar el certificado en el buscador del usuario. Las pantallas presentadas al usuario dependen del buscador que está siendo utilizado.

4.2.3 Test Certificate

Presionando este link el usuario se encuentra con una pantalla que muestra los detalles del servidor de sesión y el certificado de cliente. En la mayoría de los casos, esta pantalla únicamente mostrará los detalles del certificado de servidor web usado para asegurar la sesión (como esta pantalla no es usualmente acezada vía páginas, requiriendo autenticación del lado del cliente).

Se le ofrece al usuario la oportunidad de "Firmar" una serie de datos para probar el certificado de cliente. Al presionar el botón de "Sign" se le solicita al usuario escoger el certificado que desea usar para firmar el test de datos. Una vez que ha escogido su certificado, puede solicitársele que ingrese la frase clave asegurando sus llaves privadas (esto depende en cómo el usuario instaló el certificado y las llaves privadas durante el momento de generación de llave). Una vez que ha completado esto, los resultados del proceso de firma son mostrados.

4.2.4 Revoke Certificate

Esta pantalla da al usuario la oportunidad de revocar su propio certificado. Para hacerlo necesita llenar el formulario y presionar "continuar". El número serial del certificado puede ser obtenido examinando el certificado (usando funciones de buscador) o viendo el certificado en la lista de certificados válidos. El código CRIN fue enviado al usuario al momento de creación del certificado.

4.3 Certificates

Esta serie de opciones proveen al usuario de una lista de certificados en varios estados, válidos, expirados, revocados y suspendidos. Además proporciona una interfase para que el usuario busque un certificado.

4.3.1 Valid

Siguiendo este link el usuario se encuentra con una pantalla mostrando todos los certificados válidos. La pantalla muestra 20 certificados al mismo tiempo. El usuario puede moverse por medio de los certificados válidos usando el link "Extra References" en la parte superior derecha de la pantalla.

Para cada certificado la pantalla muestra:

Serial	El número serial del certificado
Common name	El nombre común asociado con el certificado
Issued On	La fecha y hora en que el certificado fue emitido
Email:	La dirección de email en el certificado (el usuario puede dar clic en este link para enviar el poseedor del certificado).
Role:	El tipo de certificado (e.g. Usuario)

Un usuario puede ver el contenido de un certificado dando click en el número serial del certificado que desea ver. OpenCA presenta una pantalla desplegando los detalles del certificado. En la parte inferior de esta pantalla hay dos nuevos links donde el usuario puede descargar el certificado (e instalarlo en su buscador) o iniciar el procedimiento de revocación (para hacer esto el usuario tiene que tener el número CRIN del certificado que está viendo, este número es presentado al poseedor del certificado en el momento de la creación del mismo, así que únicamente el poseedor del certificado puede revocar sus propios certificados).

4.3.2 Expired

Dando clic en este link muestra al usuario una lista de los certificados expirados. La pantalla muestra 20 certificados al mismo tiempo. El usuario puede moverse por medio de los certificados expirados usando el link “Extra References” en la parte superior derecha de la pantalla.

4.3.3 Revoked

Dando clic en este link muestra al usuario una lista de los certificados revocados. La pantalla muestra 20 certificados al mismo tiempo. El usuario puede moverse por medio de los certificados revocados usando el link “Extra References” en la parte superior derecha de la pantalla.

4.3.4 Suspended

Dando clic en este link muestra al usuario una lista de los certificados suspendidos. La pantalla muestra 20 certificados al mismo tiempo. El usuario puede moverse por medio de los certificados suspendidos usando el link “Extra References” en la parte superior derecha de la pantalla. Certificados suspendidos son aquellos que han iniciado el proceso de revocación pero que no están revocados todavía por el Certificado de Autoridad.

4.3.5 Search

Este link provee una pantalla para permitirles a los usuarios buscar un certificado en el sistema. La pantalla permite al usuario buscar basados en el criterio de nombre, email, o nombre distintivo. Son permitidos los comodines (e.g. Chris*) en cada uno de los campo. Usted no tiene que llenar cada uno de los campos para que la función de búsqueda encuentre un resultado, pero mientras más datos ingrese más exacta será la búsqueda.

4.4 Requests

Esta sección muestra solicitudes atrasadas. Pueden ser desplegadas las solicitudes de nuevos certificados y de solicitudes de revocación.

4.4.1 Certificate Requests List

Siguiendo este link el usuario se encuentra con una lista de todas las solicitudes de certificados actuales en el Registro de Autoridad. La pantalla muestra 20 solicitudes al mismo tiempo. El usuario puede moverse entre la lista usando el link “Extra References” en la parte superior derecha de la pantalla.

4.4.2 Certificate Revocation Requests List

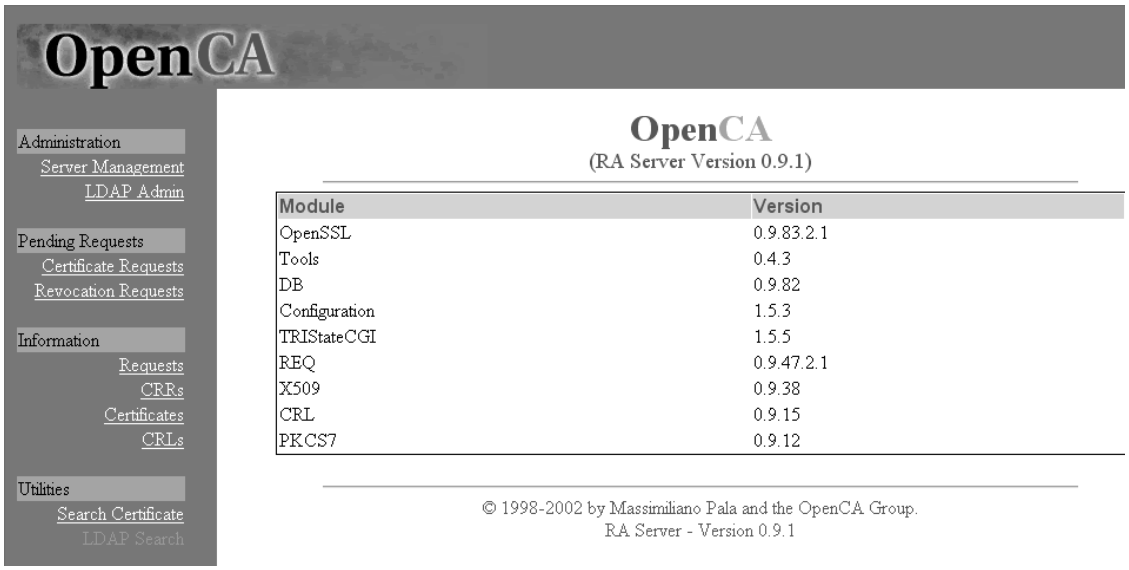
Siguiendo este link el usuario se encuentra con una lista de todas las solicitudes de revocación de certificados actuales en el Registro de Autoridad. La pantalla muestra 20 solicitudes al mismo tiempo. El usuario puede moverse entre la lista usando el link “Extra References” en la parte superior derecha de la pantalla.

MANUAL DEL ADMINISTRADOR DE LA RA

5 AUTORIDAD REGISTRADORA

Esta sección describe la interfase de autoridad de registro al OpenCA PKI. Desde estas pantallas un Administrador RA puede administrar las solicitudes de certificados, ver la información de los certificados y administrar el servidor RA.

Cada uno de los títulos abajo corresponde a una sección en el panel de menú a mano izquierda de las pantallas RA por defecto.



5.1 Administration

5.1.1 Server Management

Presionando este link lleva al usuario a la interfase RA Nodo. Desde aquí el usuario RA puede controlar el flujo de datos a y desde el RA.

5.1.2 LDAP Admin

Presionando este link lleva al usuario a la interfase de Administración LDAP. Desde aquí el usuario RA puede controlar la introducción y tachadura de datos desde el Directorio LDAP (si está configurado).

5.2 Pending Request

5.2.1 Certificate Request

Este link despliega las solicitudes sometidas por el usuario y permite al Administrador RA aprobar la solicitud.

Presionando este link despliega una pantalla principal dando al usuario una lista de quienes actúan como Autoridades de Registro. Dependiendo de la configuración "Trustcenter itself" es el de default. Dando clic en el botón de "Continue" despliega una lista de las solicitudes de certificado en la RA seleccionada.

Cada una de las solicitudes debe ser procesada en turno. Dando clic en el número serial de la solicitud, el usuario puede ver los detalles de la misma. Cuatro opciones están disponibles entonces para el Usuario RA:

5.2.1.1 Edit Request

Presionar este botón permite al usuario RA editar los detalles de la solicitud. Los campos editables son; nombre alternativo del tema (este es usualmente utilizado para la dirección de email suplida, pero puede contener otros campos), tema (o el DN) y Giro (o tipo de certificado).

5.2.1.2 Approve an Sign Request

Presionar este botón permite al usuario aprobar la solicitud y usar un certificado para firmar su aprobación. Presionando el botón al Usuario RA se le presenta una lista de certificados con los cuales firmar la aprobación de solicitud. Nota, si las solicitudes serán procesadas en el CA como un proceso secuencial, entonces cada solicitud debe ser firmada con un certificado RA válido (firmado por la Autoridad de Certificados).

5.2.1.3 Approve Request without Signing

Presionando este botón se aprueba la solicitud. Nota, esto puede ser potencialmente peligroso pues el Administrador CA tendrá que tomar una decisión de confianza para procesar la solicitud o no. Si la solicitud aprobada fue firmada por un cert RA válido, entonces esta decisión es innecesaria.

5.2.1.4 Delete Request

Presionando este botón se borra la solicitud del sistema. Hay que ser cuidadosos cuando se usa esta opción pues no hay advertencia sobre ella, la entrada es simplemente borrada.

5.2.2 Revocation Requests

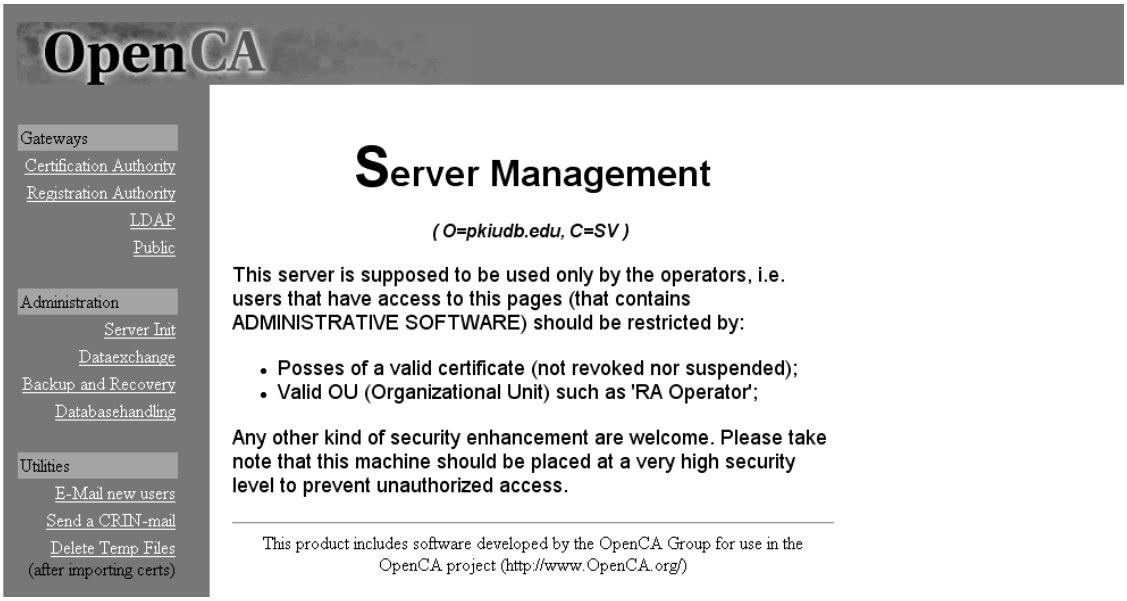
5.3 Information

Esta sección permite al usuario ver los certificados y solicitudes en todos los estados.

- Requests
- CRRs
- Certificates
- CRLs
- Utilities
- Search Certificate

6 REGISTRATION AUTHORITY NODE

El Nodo RA es la interfase usada para controlar las operaciones RA y tratar con las interfases externas, por ejemplo, exportando datos solicitados para el Certificado de Autoridad.



6.1 Gateways

Esta sección hace una lista de los componentes de OpenCA.

6.1.1 Certificate Authority

Este link lleva al usuario a la página principal del servidor CA. Este link está disponible únicamente si el CA es accesible. En la configuración normal el OpenCA está fuera de línea y entonces este link fallará.

6.1.2 Registration Authority

Este link lleva al usuario a la parte de arriba de la página de Autoridad de Registro.

6.1.3 LDAP

Esta sección lleva al usuario a una pantalla para administrar el servidor LDAP, si es que aun no ha sido configurado. Las siguientes opciones están disponibles.

6.1.4 Public

Presionando este link lleva al usuario a la interface publica OpenCA. Esta interfaz esta descrita en otra parte de este documento.

6.2 Administration

Esta sección contiene una lista de las opciones disponibles para configurar y mantener el nodo RA.

6.2.1 Server INIT

Esta pantalla es utilizada para establecer su OpenCA RA. Se espera que esta pantalla sea utilizada una sola y única ves. Aquí hay dos link:

6.2.1.1 Initialise DataBase

El administrador de la RA debería ejecutar este link para correr la lista de comando que inicializaran la base de datos. Note que si usted corre este grupo de comandos en una base de datos existentes, entonces estaría como perdiendo todos los datos existentes. Tenga cuidado.

6.2.1.2 Impot Configuration

Este link corre el proceso de importación. Requiere que exista un archivo CA de exportación en el dispositivo apropiado (o directorio). El script va abrir este archivo e importar los datos de configuración a la RA.

6.2.2 Dataexchange

Este link es utilizado para intercambiar datos con otras áreas dentro de la estructura PKI (ejemplo la CA). Dependiendo de su implementación de OpenCA únicamente algunas de las siguientes secciones van aplicar.

6.2.2.1 Enroll data to a lower lever of the hierarchy

Es poco probable que exista un nivel mas bajo de la jerarquía en el RA.

6.2.2.2 Receive Data form a lower level the hierarchy

Es poco probable que exista un nivel mas bajo de la jerarquía en la RA.

6.2.2.3 Download Data from a higher level the hierarchy

Esta sección es usada para descargar datos del CA al RA. Con el propósito de usar esta sección los datos deberías de estar exportados de la CA. Este dato es usualmente almacenado en un disquete. Si el usuario da clic en cualquiera de los siguientes link le aparecerá uno de los siguientes avisos “Necesita proveer un soporte para proceder (depende de su configuración)”, “Esta seguro de que desea continuar?”. Esto significa que necesita tener acceso de lectura al dispositivo donde están los datos exportados (por ejemplo la disquetera).

6.2.2.3.1 All

Presionando este link importa todos los datos que han sido exportados de la CA a la RA

6.2.2.3.2 Cert

Presionando este link importa únicamente los datos del certificado del CA a la RA.

6.2.2.3.3 CRLs

Presionando este link se importan los datos CRL de la CA a la RA.

6.2.2.3.4 Configuration

Presionando este link se importa únicamente los datos de configuración de la CA a la RA. Estos datos son como los roles (tipos de certificados).

6.2.2.3.5 BatchProcessors

Presionando este link importa únicamente los datos de procesos secuénciales del CA.

6.2.2.4 Upload data to higher level of the hierarchy

Esta sección le permite al administrador de la RA exportar datos para la CA. Si el usuario da clic en cualquiera de los siguientes link le aparecerá uno de los siguientes avisos “Necesita proveer un soporte para proceder (depende de su configuración)”, “Esta seguro de que desea continuar?”. Esto significa que necesita tener acceso de escritura al dispositivo donde serán escritos los datos exportados (por ejemplo la disquetera).

Nota, la exportación de datos es en la forma de un DELTA, únicamente los datos nuevos o modificados serán exportados. Es tarea del administrador modificar este comportamiento.

6.2.2.4.1 All

Presionando este link exporta todos los datos nuevos o modificados de la RA para el dispositivo de exportación.

6.2.2.4.2 Requests

Presionando este link exporta todas las solicitudes nuevas o modificadas de la RA al dispositivo de exportación.

6.2.2.4.3 CRRs

Presionando este link exporta todas las solicitudes de revocaciones nuevas o solicitadas al dispositivo de exportación.

6.2.3 Backup and Recovery

Esta sección permite al administrador de la RA respaldar y recuperar la base de datos de OpenCA RA.

6.2.3.1 BackUp DataBase

Presionando este link respalda la base de datos al dispositivo de exportación. Si el usuario da clic en cualquiera de los siguientes link le aparecerá uno de los siguientes avisos “Necesita proveer un soporte para proceder (depende de su configuración)”, “Esta seguro de que desea continuar?”. Esto significa que necesita tener acceso de escritura al dispositivo donde serán escritos los datos exportados (por ejemplo la disquetera).

6.2.3.2 Recovery Initialize DataBase

Presionando este link configura la base de datos para exportar datos. Si esta reconstruyendo la RA entonces es importante presionar este link.

6.2.3.3 OpenCA …. DB-DB if you use DBM-files

Si la base de datos RA esta basada en archivos DBM (la opción por defecto). Use este link para recuperar los datos de respaldo.

6.2.3.4 OpenCA …. DB-DB if you use a SQL – database

Si la base de datos RA esta basada en base de datos SQL (la opción preferida). Entonces use este link para recuperar los datos de respaldo.

6.2.3.5 Rebuild OpenSSL’s database and next serial number

Con el objetivo de emitir los números de solicitud de certificados a los usuarios este link debe ser presionado para que OpenCA RA reinicie su base de datos de configuración estática en los datos de la base de datos importada.

6.2.4 Database Handling

Use este link para actualizar los atributos que pueden buscarse en la base de datos después de alguna actualización de Software.

6.3 Utilities

6.3.1 E-Mail New Users

Presionando este link envía al nuevo usuario un e-mail de “bienvenida”. Estos e-mail se dicen al usuario que sus certificados están listos para la recolección y les da un link a la interfase pública para recolectar sus certificados.

6.3.2 Send a CRIN-mail

Presionando este link envía a los usuarios un correo CRIN cifrado. El correo CRIN contiene un PIN que el usuario debe usar para revocar sus propios certificados. El usuario tiene que ser capaz de descifrar el mensaje, puesto que el debió haber creado la llave privada durante el proceso de solicitud de su certificado. El mensaje es cifrado usando la llave publica en la solicitud del certificado.

6.3.3 Delete Temp Files

Este es un link a una utilidad de limpieza para borrar los archivos temporales.

7 LDAP INTERFACE

Este conjunto de pantallas controla el cargamento de datos al directorio LDAP (si hay uno configurado)

7.1 Update LDAP

7.1.1 CA-Certificate

Presionando este link carga el certificado CA al servidor LDAP. La pantalla principal muestra este proceso e indica el estado de la carga y el éxito o fracaso de la operación.

7.1.2 Certificates

Presionando este link carga los certificados actuales validos al directorio LDAP y re-mueve los certificados revocados del directorio. La pantalla principal muestra el estado e indica el éxito o fracaso de la operación.

7.1.3 CRL

Presionando este link se carga la lista de revocaciones de certificados actuales (CRL) al directorio de LDAP. La pantalla principal muestra el estado e indica el éxito o fracaso de la operación.

7.2 View CA-Certificates

7.2.1 Valid

Este link despliega una pantalla principal que muestra los certificados CA. Dando un clic en el número de serie del certificado despliega una nueva página mostrando los detalles del mismo.

Como esta página es del servidor LDAP, hay cuatro opciones LDAP relacionadas:

7.2.1.1 Add to LDAP

Escribe el certificado CA al directorio LDAP.

7.2.1.2 Add to LDAP with modified DN

Permite al usuario entrar una modificación DN al certificado y luego publicarlo en el directorio LDAP con el DN modificado.

7.2.1.3 Delete from LDAP

Borra el certificado CA del directorio LDAP.

7.2.1.4 Delete from LDAP with modified DN

Permite al usuario ingresar el nombre DN modificado antes de borrar el certificado con el DN modificado del directorio LDAP.

7.2.2 Certificates Expired

Este link despliega una lista de los certificados expirados.

7.3 View Certificates

7.3.1 Valid

Este link despliega una lista de los certificados válidos. Dando un clic en el número de serie de un certificado se despliegan los detalles del mismo.

Como esta página es del servido LDAP hay cuatro opciones LDAP relacionadas:

7.3.1.1 Add to LDAP

Presionando este botón se carga el certificado al directorio LDAP.

7.3.1.2 Add to LDAP with modified DN

Presionando este botón permite al usuario entrar un DN modificado y luego cargar el certificado al directorio LDAP con el DN modificado.

7.3.1.3 Delete from LDAP

Presionando este botón se borra el certificado del directorio LDAP.

7.3.1.4 Delete from LDAP with modified DN

Presionando este botón permite al usuario entrar un DN modificado y luego borrar el certificado del directorio LDAP con el DN modificado.

7.3.2 Expired

Este link despliega una lista de los certificados expirados. Dando un clic en el número de serie de un certificado se despliegan los detalles del mismo.

Como esta página es del servido LDAP hay cuatro opciones LDAP relacionadas:

7.3.2.1 Add to LDAP

Presionando este botón se carga el certificado al directorio LDAP.

7.3.2.2 Add to LDAP with modified DN

Presionando este botón permite al usuario entrar un DN modificado y luego cargar el certificado al directorio LDAP con el DN modificado.

7.3.2.3 Delete from LDAP

Presionando este botón se borra el certificado del directorio LDAP.

7.3.2.4 Delete from LDAP with modified DN

Presionando este botón permite al usuario entrar un DN modificado y luego borrar el certificado del directorio LDAP con el DN modificado.

7.3.3 Suspended

Este link despliega una lista de los certificados suspendidos. Dando un clic en el número de serie de un certificado se despliegan los detalles del mismo.

Como esta página es del servido LDAP hay cuatro opciones LDAP relacionadas:

7.3.3.1 Add to LDAP

Presionando este botón se carga el certificado al directorio LDAP.

7.3.3.2 Add to LDAP with modified DN

Presionando este botón permite al usuario entrar un DN modificado y luego cargar el certificado al directorio LDAP con el DN modificado.

7.3.3.3 Delete from LDAP

Presionando este botón se borra el certificado del directorio LDAP.

7.3.3.4 Delete from LDAP with modified DN

Presionando este botón permite al usuario entrar un DN modificado y luego borrar el certificado del directorio LDAP con el DN modificado.

7.3.4 Revoked

Este link despliega una lista de los certificados revocados. Dando un clic en el número de serie de un certificado se despliegan los detalles del mismo.
Como esta página es del servido LDAP hay cuatro opciones LDAP relacionadas:

7.3.4.1 Add to LDAP

Presionando este botón se carga el certificado al directorio LDAP.

7.3.4.2 Add to LDAP with modified DN

Presionando este botón permite al usuario entrar un DN modificado y luego cargar el certificado al directorio LDAP con el DN modificado.

7.3.4.3 Delete from LDAP

Presionando este botón se borra el certificado del directorio LDAP.

7.3.4.4 Delete from LDAP with modified DN

Presionando este botón permite al usuario entrar un DN modificado y luego borrar el certificado del directorio LDAP con el DN modificado.

7.4 View CRLs

7.4.1 CRLs

Este link despliega una lista de la lista de revocación de certificados (CRLs). Dando un clic en el Ver (***este es un insecto, Yo pienso que debería dar clic en el número de serie del CRL ***) del CRL despliega la lista de detalles CRL de los certificados revocados.

Dando un clic en el número de serie de un certificado revocado despliega la pantalla de detalles del certificado en la misma forma que presionando el link “Ver Certificados Válidos”.

Como esta página es del servidor LDAP hay dos opciones relacionadas:

7.4.1.1 Add to LDAP

Presionando este botón adjunta el CRL al directorio LDAP.

7.4.1.2 Add to LDAP with modified DN

Presionando este botón permite al usuario cambiar los detalles del emisor antes de cargarlos al directorio LDAP.