Universidad Tecnológica de Panamá

Facultad de Ingeniería de Sistemas Computacionales

Licenciatura en Ingeniería de Sistemas de Información

Seguridad Informática

Laboratorio No. 2

Tema:

“Práctica de Open CA”

Presentado por:  
Gabriel Díaz 20-53-5198

Jonathan Gamero 8-982-2008

Fernando Cutire 8-972-906

Grupo: 1IF-141

A consideración de:

Ing. José Moreno

2022

# RESUMEN

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.

# ÍNDICE

[RESUMEN i](#_Toc104670091)

[ÍNDICE ii](#_Toc104670092)

[INTRODUCCIÓN 1](#_Toc104670093)

[DESARROLLO 2](#_Toc104670094)

[1. PARTE 1. Solicitando un Certificado Digital 2](#_Toc104670095)

[2. PARTE 2. Configurando la CA 5](#_Toc104670096)

[3. PARTE 3. Exportación e importación del CA. 17](#_Toc104670097)

[CONCLUSIONES 23](#_Toc104670098)

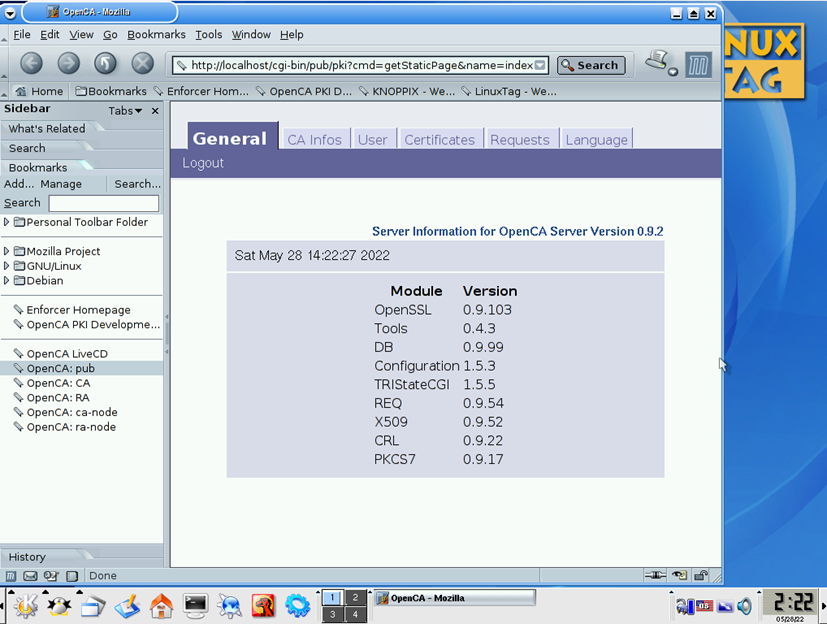
[REFERENCIAS BIBLIOGRÁFICAS 25](#_Toc104670099)

# INTRODUCCIÓN

Una **autoridad de certificación (CA)**, también a veces referido como **autoridad de certificación**, es una empresa u organización que actúa para validar las identidades de las entidades (como sitios web, direcciones de correo electrónico, empresas o personas individuales) y vincularlas a claves criptográficas mediante la emisión de documentos electrónicos conocidos como “Certificados digitales” [1].

# DESARROLLO

## PARTE 1. Solicitando un Certificado Digital

1. 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. 
2. Realice un clic en “CA Infos”

Interfaz de usuario gráfica

Descripción generada automáticamente

1. Instale el Certificado Raíz de la Autoridad de Certificación

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. Comente la importancia de este paso. Seleccione la opción que más se adecue al navegador que está utilizando.

R/: El caso elegido fue Mozilla, ya que es el navegador predefino que se está utilizando.

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

1. ¿Falló el paso? Comente por qué. No pase a la siguiente hoja hasta que haya llenado en el espacio que sigue porqué fallo este paso. Recuerde pensar como administrador del sistema.

R/: No se puede obtener un certificado de autoridad por la entidad, en este caso OpenCA no se ha emitido certificados disponibles para dicha distribución en la base de datos. Por lo tanto, habrá primero que generar los certificados para luego poder obtenerlos.

## 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.

Interfaz de usuario gráfica

Descripción generada automáticamente

1. 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.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

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

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. 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.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. 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.

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. 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.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

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

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

6.2 Revisemos ahora en nuestro browser el certificado instalado.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente con confianza media

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.

1. 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.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica

Descripción generada automáticamente

## PARTE 3. Exportación e importación del CA.

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

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Tenemos el Certificado del Operador CA. Mire los detalles:

Texto

Descripción generada automáticamente

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.)

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

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)

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

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

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

Podemos ver las características del certificado instalado.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

# CONCLUSIONES

En esta práctica de laboratorio, se creó una de certificación privada usando una distribución de Linux (Knoppyx) como servidor independiente de OpenCA. Aprendió cómo se generan un CA. Se creó y firmó una solicitud de firma de certificado (CRT) para importarlo en el navegador web, luego, se realizó un acceso de administrador de certificados.

# REFERENCIAS BIBLIOGRÁFICAS

|  |  |
| --- | --- |
| [1] | ssl, «ssl,» ssl.com, [En línea]. Available: https://www.ssl.com/es/preguntas-frecuentes/%C2%BFQu%C3%A9-es-una-autoridad-de-certificaci%C3%B3n%3F/. [Último acceso: 25 05 2022]. |