Universidad de Buenos Aires

Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Certificación Cruzada
Confianza entre organizaciones

Autor:

Edy Javier Milla Reyes
Cohorte 2012

Tutor de Trabajo Final:

Ingeniero Hugo Pagola

Fecha de presentación

11 de octubre de 2013

Declaración jurada

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente (v.8.6) y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO

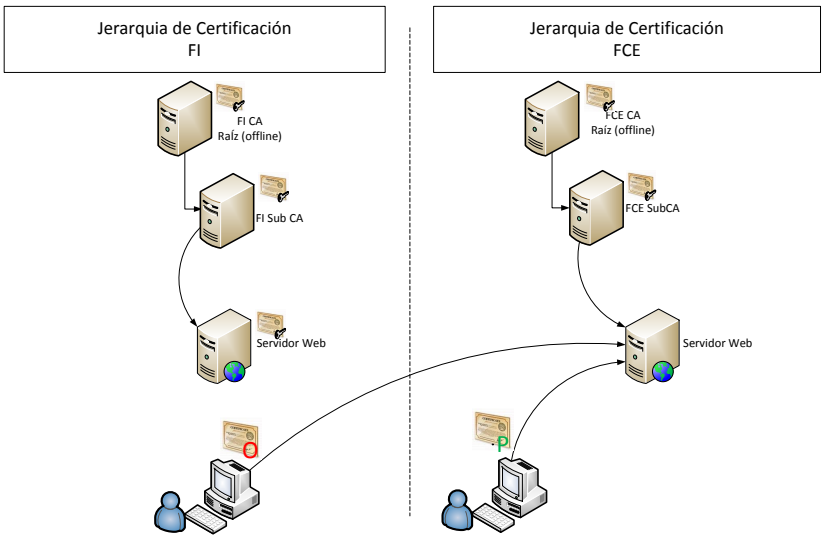
Edy Javier Milla Reyes

No. Documento 14392

Resumen

En el presente trabajo, se expone el modelo de Certificación Cruzada como una solución para establecer confianza entre organizaciones que cuentan con sus Infraestructuras de Clave Pública (PKI). De esta forma, se extiende su uso para establecer una relación de confianza utilizando certificados digitales cruzados entre ellas. Se plantea una prueba de concepto utilizando los sistemas operativos Windows Server 2008 y Linux Debian OpenSSL, cada cual representa una organización. Se han establecido Autoridades Certificantes (AC) raíz y subordinadas con dos niveles jerárquicos, el primer nivel representa la AC raíz y el segundo nivel la AC subordinada.

Para una mejor comprensión, se ha creado un escenario donde se plantea que el personal de la Facultad de Ingeniería (FI), desea intercambiar información con la Facultad de Ciencias Económicas (FCE). La FCE tiene a cargo el sistema de presupuesto de la UBA en un portal WEB, por lo que personal de la FI, accede para consultar y modificar las partidas presupuestarias. En la siguiente ilustración se muestra una representación gráfica del ambiente.



En la prueba de concepto, la certificación cruzada se realiza en el segundo nivel de la jerarquía entre las AC subordinadas, La FI firma el certificado del certificado de la AC Subordinada de la FCE, estableciendo de esta manera la relación de confianza. El certificado cruzado se emite incluyendo políticas que se establecen de acuerdo a las necesidades o nivel de la confianza que se desea lograr.

Lo presentado, es parte de una solución de seguridad, y no una solución completa en si misma que abarque todos los aspectos de seguridad en las organizaciones.

Este mismo trabajo, ha sido enviado a manera de artículo a TIBETS 2013, siendo aceptado para su presentación en el taller a realizarse en octubre de este mismo año. En el anexo se incluye el artículo enviado.

Palabras clave: Certificación Cruzada, Confianza, Autoridades Certificantes, Certificados Digitales, Modelos de Certificación.

Tabla de contenido

Declaración jurada iii
Resumen iv
Agradecimientos ix
Nómina de abreviaturas x
Introducción 1
Objetivos 3
Alcance 4
Estructura 5
Enfoque 5
Relevancia 6
I Confianza entre organizaciones 7
1.1 Confianza 7
1.2 Elementos importantes para establecer confianza 8
1.3 PKI como solución tecnológica para establecer confianza 11
1.4 Componentes de la Infraestructura de Clave Pública 11
1.5 Certificados digitales 12
1.6 Autoridades Certificantes 13
1.7 Listas de revocación de certificados 13
II Modelos de Confianza 14
2.1 Modelo Jerárquico 15
2.3 Interoperabilidad de certificados PKI 18
2.4 Elementos requeridos para la implementación de un modelo de certificación cruzada. 19
III Proceso de certificación cruzada 21
3.1 Creación de la plantilla del Agente para la solicitud de firmado (req) 22
3.2 Incorporación de las plantillas de certificación cruzada a la lista de emisión de certificados 23
3.3 Emisión del certificado Cross Certification Enrollment Agent 24
3.4 Creación y parametrización del archivo de políticas de certificación 25
3.5 Firmado de la solicitud del certificado (req) 27
3.6 Emisión del Certificado Cruzado 28
3.7 Verificación de las propiedades del certificado cruzado 28

3.8 Distribución de la cadena de certificación 29
3.9 Consideraciones que se deben tomar en cuenta al momento de implementar este modelo 30
3.10 Procedimiento para la gestión de los certificados digitales que se han cruzado. 31
3.11 Mejores prácticas para la gestión de certificados digitales cruzados 33
3.12 Prueba de concepto de la solución 33
3.13 Problemas encontrados en el proceso 34
Conclusiones 36
Glosario 38
Bibliografía Específica 41
Bibliografía General 43
Anexos 44
Laboratorio 1: Creación de una autoridad certificante (CA) subordinada integrada con Active Directory Domain Services (ADDS). 44
Objetivo 44
Autoridad Certificante Subordinada Integrada 44
Proceso de creación de la autoridad certificante subordinada integrada con ADDS en Windows server 2008 45
Proceso de firmado de la CA integrada 54
Verificaciones del proceso de instalación de la CA operacional 61
Laboratorio 2: Creación de una autoridad certificante (AC) Raíz y AC subordinada en Linux para la FCE. 64
Objetivo 64
Proceso de creación de la autoridad certificante raíz 65
Proceso de creación de la autoridad certificante subordinada 66
Proceso de creación de un certificado de servidor 67
Proceso de configuración del Apache para una conexión SSL 68
Laboratorio 3: Proceso de Certificación Cruzada entre la Autoridad Certificante (CA) Subordinada Integrada con ADS FI y CA subordinada Linux OpenSSL FCE. 71
Objetivo 71
Creación de la plantilla del Agente para la solicitud de firmado (req) 71
Incorporación de las plantillas de certificación cruzada a la lista de emisión de certificados 77

Emisión del certificado Cross Certification Enrollment Agent 78
Preparación y creación del archivo de políticas (policy.inf) 80
Proceso de emisión del certificado cruzado 84
Emisión del Certificado Cruzado 85
Verificación de las propiedades del certificado cruzado 86
Distribución de la cadena de certificación. 88
Scripts utilizados para la generación de certificados con OpenSSL 91
CA Raíz de FCE 91
CA Subordinada de FCE 94
Generación de certificado SSL utilizado para servicio web FCE 98
Generación de certificado para correo electrónico FCE 99
Articulo Laboratorio de confianza entre organizaciones utilizando Certificación Cruzada a TIBETS 2013 100
Carta de aceptación VII Congreso Iberoamericano de Seguridad Informática 107

Agradecimientos

El presente trabajo está dedicado primeramente a Dios, por permitir el desarrollo académico y profesional en esta etapa de mi vida. A mi esposa por el continuo apoyo y la paciencia que ha demostrado a pesar de no estar a mi lado al encontrarnos distantes en países diferentes. Mis hijos por ser la razón de haber tomado la decisión de continuar con mis estudios académicos y ser ejemplo para ellos, motivándoles a la vez para que se dispongan a cumplir las metas que se propongan en la vida.

A la administración superior de la institución que represento, Banco Central de Honduras, por haber confiado la oportunidad de este desarrollo académico y profesional, demostrando a la vez su compromiso de contar con profesionales altamente capacitados en lo referente a la seguridad de la información.

A mi asesor académico Ingeniero Hugo Pagola por su continuo apoyo y paciencia en la revisión de este texto.

Al cuerpo docente, administrativo y demás personal de la Universidad de Buenos Aires, quienes han proporcionado todos los medios a su alcance para el continuo desarrollo de la Carrera de Especialización en Seguridad de la Información.

A todas aquellas personas que directa o indirectamente han contribuido con sus esfuerzos para el logro de este objetivo.

Nómina de abreviaturas

AICPA/CICA	American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants
API	Application Program Interface
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
CA	Certification Authority (Autoridad Certificante)
CC	Cross Certification (Certificación Cruzada).
CN	Common Name (Nombre Común).
DNS	Domain Name Systen
EE	End Entity (Entidad final)
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IP	Internet Address
ITU	International Telecommunications Union
MD	Message Digest (Resumen de mensaje, digesto)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infraestructure (Infraestructura de Clave Pública).
RDN	Relative Distinguished Name
RFC	Request for Comments
UPN	User Principal Name
URI	Uniform Resource Identifier

Introducción

El presente documento es una extensión del trabajo final de la materia Seguridad en Redes I. En esa ocasión, el tema desarrollado manifestó en mi persona un particular interés en seguir investigando, por lo que éste fue seleccionado como tema para el trabajo final de la Carrera de Especialización en Seguridad informática.

Debido a que las organizaciones cada día estrechan sus relaciones de negocio para ofrecer sus productos y servicios a los clientes y así mismo, la amplia utilización de sistemas informáticos que potencian las actividades de negocio, éstos se han convertido en un eje central que impulsan la interacción del intercambio de la información entre las organizaciones. A la vez, se requiere que las organizaciones consideren modelos (que en la actualidad se encuentran disponibles) para asegurar que la información sea manejada de tal forma que se garantice razonablemente la confidencialidad, integridad, disponibilidad y no repudio (entre otros).

Para atender estos desafíos, se ha investigado acerca del uso de certificados digitales, particularmente el modelo de Certificación Cruzada (CC), que permite a las organizaciones que ya cuentan con una Infraestructura de Clave Pública (PKI), para que ésta misma sea aprovechada extendiendo su uso para establecer niveles de confianza, permitiendo el intercambio de información de forma segura. Los certificados digitales cruzados son ajustados mediante parámetros de acuerdo a las políticas establecidas para el uso de un servicio (producto de la relación de negocios). Por ejemplo, una de las organizaciones requiere que únicamente sean aceptados los certificados que fueron emitidos a la unidad organizativa finanzas, rechazando el resto.

Para facilitar la comprensión de este modelo, se presenta una situación en la cual dos organizaciones representadas por las Facultades de

Ingeniería (FI) y Ciencias Económicas (FCE) de la Universidad de Buenos Aires, desean intercambiar información de forma segura. Por lo que han decidido efectuar el intercambio de información utilizando certificados digitales cruzados, logrando de esta manera la interoperabilidad de sus sistemas.

A manera de material educativo, este documento fue presentado en el Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información (TIBETS) en su edición 2013 en formato de artículo que muestra su desarrollo como experiencia de laboratorios para ser utilizado en la materia Seguridad en Redes I, mismo que fue aceptado para su presentación en el congreso a realizarse en octubre del presente año (carta de aceptación consta en los anexos). TIBETS, es un espacio para que profesores y alumnos intercambien experiencias docentes y discentes en el marco de la seguridad de la información, nuevos enfoques, propuestas y tendencias en la educación de la seguridad informática. En el anexo se incluye una copia del artículo presentado.

También, se ha aprovechado en la materia Seguridad en Redes I del posgrado en Seguridad Informática, para que los estudiantes pongan en práctica los laboratorios con el objetivo que desarrollen o consoliden su conocimiento en estos temas.

Objetivos

Los siguientes objetivos se han planteado en la realización del presente documento:

- Presentar un marco teórico que permita ubicar el contexto del tema.
- Presentar los modelos de confianza utilizando certificados digitales.
- Mostrar los elementos requeridos para la implementación de un modelo de Certificación Cruzada (CC) que pueda ser utilizado por organizaciones que cuentan con una Infraestructura de Clave Pública (PKI).
- Mostrar las consideraciones que se deben tomar en cuenta al momento de implementar este método.
- Proveer un procedimiento para la gestión de los certificados digitales que se han cruzado.
- Proveer mejores prácticas para la gestión de certificados digitales cruzados.
- Efectuar una prueba de concepto de la solución.
- Documentar los problemas encontrados en el proceso.

Alcance

- El marco teórico únicamente contiene la información suficiente para exponer los temas de confianza, certificación cruzada e interoperabilidad.
- De acuerdo al escenario propuesto (Certificados Cruzados entre la FCE y FI) emitir certificados cruzados aplicando reglas de restricción de nombres y aplicación en el certificado subordinado emitido por la CA de la FCE para ser utilizados en la red de la FI.
- Presentar una prueba de concepto utilizando el modelo de certificación cruzada permitiendo el intercambio de información de forma segura (relativamente) entre organizaciones.
- No es parte del alcance explicar cómo establecer una Infraestructura de Clave Pública (PKI), sin embargo se explican algunos componentes.

En la prueba de concepto el alcance se delimita al cumplimiento de las siguientes actividades:

- Configurar dos ambientes con el servicio de Infraestructura de Clave Pública (PKI) utilizando Windows Server 2008 y Linux Debian OpenSSL. Cada ambiente representa una organización.
    - Facultad de Ingeniería (FI) → Windows Server 2008
    - Facultad de Ciencias Económicas (FCE) → Linux Debian OpenSSL.
- Preparar varios archivos de políticas que servirán de base para delimitar las funcionalidades del certificado cruzado.
- Llevar a cabo el proceso de certificación cruzada.
    - Emitir certificados cruzados utilizando diversos valores en la extensión de Nombre Común (CN) u otras extensiones.
- Configurar un servidor de aplicaciones WEB que permita poner a prueba los certificados cruzados que fueron emitidos.

Estructura

Este documento está estructurado en tres capítulos, en el primero trata temas relativos a la confianza, generalidades de infraestructuras de clave pública y de certificados digitales. En el segundo se muestran los modelos para establecer confianza utilizando certificados digitales en las organizaciones y el tercero muestra el proceso de certificación cruzada. En los anexos se encuentra los laboratorios que permiten experimentar el modelo citado. Los procedimientos a efectuar en el sistema operativo Windows y Linux Debian Utilizando OpenSSL, demuestra que se puede lograr la interoperabilidad entre los certificados que son emitidos por estas plataformas.

Enfoque

Para una mejor comprensión de este modelo, se han preparado una serie de laboratorios que permiten llevar a cabo el proceso de certificación cruzada entre dos organizaciones que desean intercambiar información. Cada una cuenta con su propia PKI (cada una con su propia CA Raíz), al no tener una CA Raíz común, deben recurrir al proceso de certificación cruzada que además, les permite seleccionar los certificados que han de ser aceptados de su contraparte y no todos los certificados como ocurriría si se intercambian los certificados raíz y subordinados (intermedios), limitando de esta manera la cantidad de certificados validos en esta relación.

Relevancia

Debido a que las organizaciones tienen que intercambiar información para el desarrollo exitoso de sus negocios, la relevancia de este tema representa un particular interés en aquellos que quieren efectuar este intercambio de forma segura. Las nuevas necesidades de negocio, regulaciones y cumplimiento de normativas, en ocasiones obligan a las organizaciones a implementar Infraestructuras de Clave Pública (PKI). Aprovechando esta necesidad, el modelo de certificación cruzada puede ser utilizado para que dos o más organizaciones puedan interactuar, permitiéndoles restringir los certificados que se pueden aceptar.

Así mismo, se proporcionan laboratorios detallados a manera de prueba de concepto para aquellos que quieran experimentar el modelo de certificación cruzada en entornos Windows y Linux.

También los laboratorios son adecuados para la instrucción en el aula de clases, permitiendo que los estudiantes ensayen este tema con el objetivo de poner en práctica los conocimientos adquiridos en las clases teóricas.

I Confianza entre organizaciones

Objetivo de este capítulo: Definir algunos conceptos de confianza, confianza en las organizaciones, presentar algunos elementos importantes para obtener confianza. PKI como solución tecnológica para establecer confianza. Enunciar los componentes de una PKI.

1.1 Confianza

La nueva palabra de moda (buzzword) para el siglo veintiuno es: “confianza” [1]. Se habla mucho de confianza en nuestro entorno cotidiano, confianza en la fabricación de productos que se consumen, confianza en los servicios que se brindan y confianza en las operaciones que se intercambian entre entidades.

La RAE define confianza como [2]: “Seguridad que alguien tiene en sí mismo”, en el presente documento se habla de confianza entre organizaciones, por lo que este concepto se amplía a: “Seguridad que una organización tiene en sí misma, que el intercambio de información que se efectúa hacia otra organización se ha operado de forma segura”.

En el mundo digital en que vivimos, la confianza debe aplicarse de acuerdo al contexto de las organizaciones. El riesgo de pérdida de información debido al uso de sistemas informáticos es extremadamente alto y en un solo incidente relacionado con el uso de tecnologías de información se pueden experimentar grandes pérdidas de datos. De acuerdo a los reportes publicados por DataLossDB.org (DataLossDB es un proyecto de investigación que tiene como propósito documentar y reportar los incidentes relacionados con la perdida de datos a nivel mundial), cada incidente revela una pérdida de información importante (>6000 registros). En el último incidente reportado por Facebook Inc. Seis millones de registros fueron expuestos [3].

Lo anterior provoca que las organizaciones estén expuestas a una serie de consecuencias como disminución en la confianza y reputación. Por lo tanto, esto implica que los controles relacionados con el nivel de confianza entre entidades que intercambian información deban ser elevados.

El nivel de confianza varía dependiendo del enfoque al cual se aplica (contexto). Los elementos de control que se establecen en una operación financiera de alto valor, difiere de los controles que se aplican a operaciones de bajo valor. Cada organización, debe definir los controles más apropiados de acuerdo a la política y criterio de clasificación de la información que se ha analizado del contexto.

1.2 Elementos importantes para establecer confianza

De acuerdo a Raina Kapil [1] la confianza tiene tres elementos importantes:

> ***Predictibilidad**: la habilidad para producir consistentemente un resultado (positivo) esperado, evita en el cliente la necesidad de mantener constantemente un alto grado de vigilancia. La seguridad, servicio y calidad de las organizaciones, al ser más predecible, mayor facilidad que el cliente adquiera (consuma) sus servicios.*
>
> ***Activos**: La confianza no es un factor importante, a menos que haya activos (físicos o lógicos) importantes en riesgo de pérdida o daño. A mayor valor, se requiere un nivel mayor de confianza. Sitios web como eBay (un sitio de subastas en línea), utiliza socios de servicios de custodia para las operaciones de mayor valor (generalmente más de EE.UU. $ 500) como un método para aumentar la confianza en las transacciones entre dos personas desconocidas.*

> ***Incertidumbre**: La confianza se requiere, cuando hay un grado de incertidumbre en la capacidad de verificar una operación o resultado. En general, si toda la información se conoce sobre las partes y la transacción, entonces se reduce en gran medida la necesidad de confianza. Sin embargo, la mayoría de las transacciones, presentan un nivel de incertidumbre, incluyendo la historia desconocida del comprador o vendedor, la calidad desconocida de servicios o productos, y así sucesivamente.*

Considere el siguiente caso, cuando una organización deposita en su almacén de autoridades de certificación raíz de confianza y en el almacén de autoridades de certificación intermedias los certificados que pertenecen a la jerarquía de la CA Symantec/Verisign, los certificados emitidos por esta CA pasan a ser certificados de confianza, incluso los emitidos para otras organizaciones. Esta empresa ha ganado un gran nivel de confianza entre las organizaciones por lo que éstas y muchos individuos confían sus certificados emitidos.

De esta manera, los usuarios de servicios que utilizan certificados emitidos por Symantec/Verisign, al ver un resultado consistente (predictibilidad), la protección de los recursos (activos) en riesgo de pérdida y al ofrecer la capacidad de verificar la identidad de las partes (bajar la incertidumbre), genera un alto grado de confianza.

También La confianza se logra cuando las organizaciones forman parte de iniciativas que buscan fortalecer la seguridad de los entornos en Internet, Symantec/Verisign, DigiCert, Inc. y Comodo CA Ltd (entre otros) son miembros de The Certification Authority Browser Forum [4], una organización voluntaria que aglutina a los líderes en autoridades certificantes y vendedores de navegadores de internet y otras aplicaciones. Los miembros que tienen una CA emisora de certificados o una CA Raíz deben cumplir con la auditoria para CAs: WebTrust (AICPA/CICA), ETSI 102042 o ETSI 101456 [5] para poder incluir sus certificados en los navegadores web.

En el ámbito financiero, la ISO 21188 establece un marco de requisitos para la gestión de una PKI a través de las políticas de los certificados y declaraciones de prácticas de certificación en el sector de servicios financieros.

Como podemos observar, si queremos implementar ámbitos tecnológicos que generen confianza, se debe recurrir a elementos apropiados que permitan visualizar entornos seguros y que garanticen su efectividad en las organizaciones.

1.3 PKI como solución tecnológica para establecer confianza

La Infraestructura de Clave Pública (PKI) [6], es una combinación de software, tecnologías de cifrado, y servicios que permiten a las organizaciones proteger la seguridad de sus comunicaciones, y sus operaciones de negocio. PKI integra certificados digitales, criptografía de clave pública, y autoridades certificantes dentro de una arquitectura de seguridad en la red de toda la organización. La PKI de una organización típicamente incluye la emisión de certificados digitales a entidades finales (EE).

El RFC 2828 [pagina 136] en su Glosario Seguridad en Internet define PKI como un sistema compuesto por CAs (y, opcionalmente, Autoridades de Registro RAs y otros servidores de soporte y agentes) que efectúan tareas de administración de certificados, gestión de archivos, gestión de claves y funciones de gestión de tokens dirigido a una comunidad de usuarios para aplicaciones de criptografía asimétrica.

1.4 Componentes de la Infraestructura de Clave Pública

Las organizaciones implementan ambientes de PKI para establecer confianza en sus entornos. Si esta PKI se diseña de acuerdo a lineamientos, marcos normativos y estándares, ésta implementación gozara de plena confianza de los usuarios y organizaciones que tienen relación con la infraestructura.

Dependiendo de la complejidad de las necesidades de las organizaciones, los componentes de una PKI pueden variar. Básicamente se encuentran los siguientes:

- Certificados Digitales
- Autoridades Certificantes
- Listas de revocación de certificados

1.5 Certificados digitales

Los certificados [6] son el fundamento de una PKI. Son representaciones digitales de usuarios, computadoras, dispositivos de red o servicios, estos últimos denominados como entidad final (EE). Éstos son respaldados por una autoridad certificante (CA). Tienen asociado un par de claves denominadas pública y privada. Únicamente la clave pública se almacena en el certificado en la extensión “public key”.

Contienen una colección de información (generalmente de 2 a 4 kilobytes) digitalmente firmada y típicamente incluyen lo siguiente:

- Información acerca de la EE (identificado por la extensión subject) que es dueño de las claves pública y privada.
- Información acerca del emisor (CA).
- La clave pública correspondiente al par de claves asociadas al certificado (en el certificado no está contenida la clave privada).
- Los nombres de los algoritmos de cifrado y digesto soportados por el certificado.
- Un listado de extensiones del estándar ITU X.509.[1]
- Información que permite determinar el estado de revocación y validez del certificado.

Para emitir un certificado digital, se debe asegurar la identidad del solicitante. Similar a un documento de identificación personal, el emisor debe solicitar la documentación que considere pertinente para identificar al EE.

Cuando se emite un certificado digital, la CA firma digitalmente el certificado con su clave privada. Esta firma certifica que el certificado fue firmado por la CA emisora y ayuda a determinar si ha habido cambios

[1]La serie X está destinada a los temas de Redes de datos, comunicaciones de sistemas abiertos y seguridad.

después de la emisión. Cualquier cambio provoca que el certificado sea inválido al comprobar la firma utilizando la clave pública de la CA emisora.

1.6 Autoridades Certificantes

Emiten certificados y usualmente listas de revocación de certificados (CRLs). También efectúan una serie de tareas administrativas Las CA, que generalmente son delegadas en las Autoridades de Registro.

Validar la identidad de un solicitante del certificado digital, emisión del certificado una vez comprobada la identidad de solicitante hasta gestionar la revocación del certificado (en el caso de compromiso de la clave privada) son algunas de las funciones que desempeña una CA.

Algunas organizaciones implementan más de una CA con el propósito de mejorar la gestión de los certificados. Las CAs se organizan en jerarquías iniciando por una raíz y varias subordinadas que pueden ejercer diversas funciones e incluso estar destinadas a generar tipos de certificados para determinados fines.

1.7 Listas de revocación de certificados

Debido a que los certificados están expuestos a una serie de riesgos, debe existir un mecanismo de revocación que permita informar a los usuarios de la PKI que un certificado ha sido comprometido. La lista de revocación de certificados o CRL es generado por la CA, es un archivo que contiene los números de serie, fecha y razón de revocación de los certificados que han sido reportados por las EE. Este archivo se publica periódicamente y las aplicaciones que utilizan los certificados deben consultar esta lista antes de efectuar cualquier operación con el propósito de comprobar su estado (si aparece en la lista, el certificado ha sido revocado).

II Modelos de Confianza

Objetivo de este capítulo: mostrar los modelos de confianza en infraestructuras de clave pública, interoperabilidad de certificados digitales emitidos por distintas plataformas y requerimientos para efectuar certificación cruzada.

Cuando las organizaciones crean sus PKI, la confianza solamente se establece en los certificados emitidos por su propia PKI. La interacción entre organizaciones, crea la necesidad para que el marco de confianza interno sea extendido, logrando de esta manera establecer confianza para el uso de aplicaciones entre ellas, por ejemplo un servidor web, aplicaciones firmadas, etc.

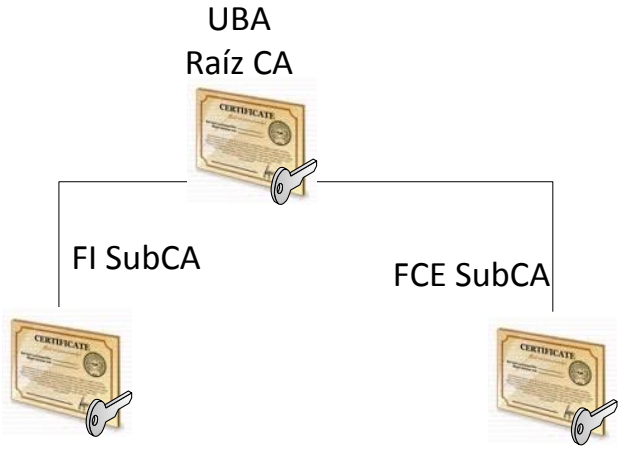
Una vez que se han cubierto los requisitos legales, acuerdos de uso, acuerdos de nivel de servicio (SLA), procedimientos de operación, etc. Las organizaciones pueden recurrir a los siguientes modelos para establecer confianza entre sus PKI:

- Modelo Jerárquico
- Modelo Certificación Cruzada

Cada modelo es detallado en las siguientes secciones, en el presente trabajo, se detalla el modelo de certificación cruzada ya que éste permite que se establezca la confianza entre organizaciones que ya tienen establecidas sus PKI. De esta manera no es requerido generar CA’s nuevamente para establecer un punto de confianza.

2.1 Modelo Jerárquico

En este modelo, el punto de confianza inicia en la CA Raíz, por consiguiente, todas las CAs que sean firmadas por esta CA forman parte de una jerarquía de confianza. En nuestro escenario, para que exista confianza entre las CAs de la FI y la FCE, se debe establecer una CA Raíz que sea común para estas dos organizaciones. En la siguiente figura se muestra el modelo planteado:

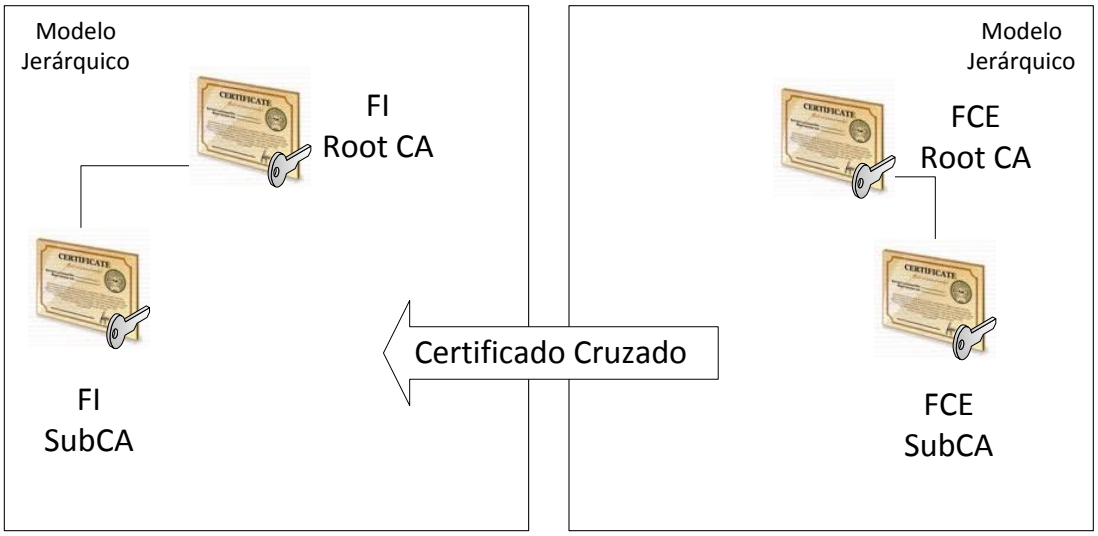


La “UBA Raíz CA” representa la CA común para la CA de la FI y FCE (denominadas subordinadas por depender del CA Raíz), Al existir una CA común, todos los certificados emitidos por “FI SubCA” son de confianza para la FCE y viceversa. Si se quiere implementar este modelo en organizaciones que tienen sus PKI operando con CAs Raíz diferentes (CA Raíz y CA subordinadas con certificados emitidos para diversas aplicaciones), implica que se deben revocar todos los certificados emitidos de sus aplicaciones, servicios y usuarios, y establecer nuevamente las CAs necesarias junto con los certificados requeridos para operar nuevamente. Además, una vez establecida la relación, se deben definir restricciones (constraint) adecuadas para limitar los certificados que la FI SubCA va a permitir utilizar de la FCE SubCA en su entorno de confianza. Si a futuro se rompe la relación de negocios, esto provocaría que las empresas deban volver a revocar todos sus certificados y volver a generar CAs individuales. El otro problema que se

visualiza es tomar la decisión de ubicar físicamente la CA Raiz, ¿debe estar en la FCE o en la FI?.

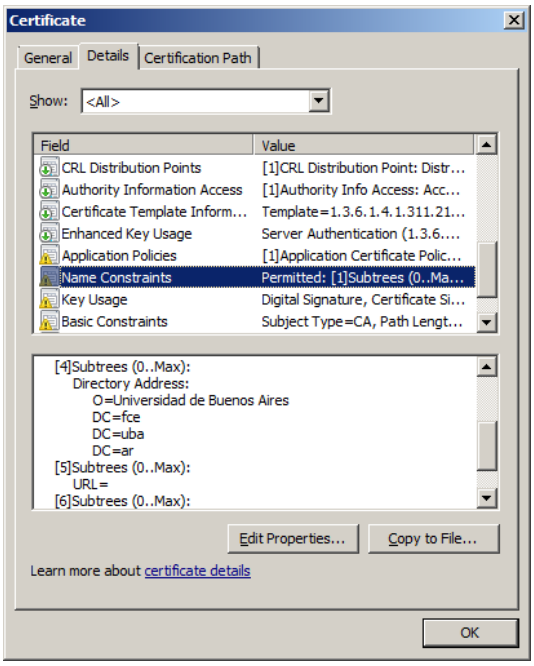
2.2 Modelo Certificación Cruzada

En este modelo, cada organización tiene una estructura jerárquica (2.1) por lo que no se tiene ninguna vinculación entre ellas (salvo el certificado cruzado). Este modelo permite que estas dos (o más) organizaciones puedan establecer el punto de validez de su asociado, firmando el certificado del nivel que se desee. En la representación gráfica se muestra que las dos organizaciones tienen su propia jerarquía, la FCE envía el certificado de la SubCA a la jerarquía de la FI (ambas en el segundo nivel). La SubCA de la FI al firmar éste certificado el cual tiene además reglas de nombre y de aplicación el certificado resultante pasa a ser un certificado de la jerarquía de la FI.



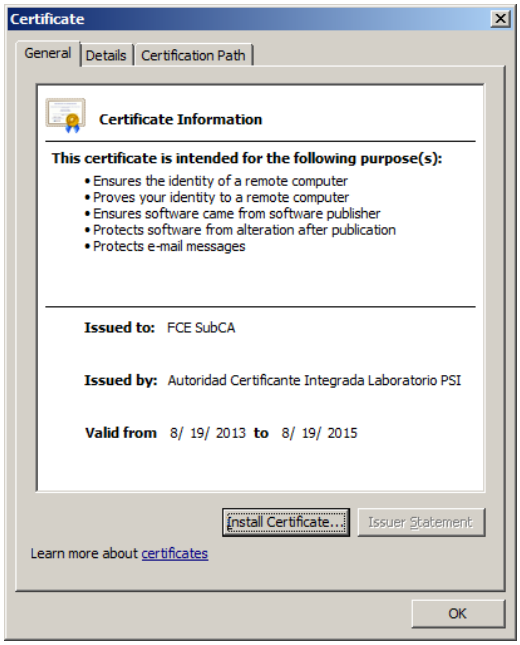
Cuando las APIs criptográficas del sistema operativo reciben la solicitud de comprobación de un certificado EE emitido por la FCE, éstas construyen la cadena de certificación incluyendo el certificado cruzado que al hacer sido firmado por la SubCA de la FI pasa a ser un certificado de confianza. (el certificado cruzado debe guardarse en el almacén de certificados intermedios de confianza).

Las APIs criptográficas comprueban además que Los certificados de EE de la FCE cumplan con las reglas de nombre o aplicación definidas en el proceso de certificación cruzada.



En la siguiente representación gráfica se muestra que las reglas de aplicación utilizadas a este certificado cruzado, corresponden a los OID

1.3.6.1.5.5.7.3.1 para autenticación de servidor, 1.3.6.1.5.5.7.3.2 para autenticación de cliente, 1.3.6.1.5.5.7.3.3 para autenticación de código y 1.3.6.1.5.5.7.3.4 para autenticación en email.



2.3 Interoperabilidad de certificados PKI

El estándar ITU-T X509 que define el formato de certificados digitales, permite que los fabricantes que soportan esta tecnología, apegarse a lineamientos, reglas, formatos, etc. establecidos con el fin de garantizar la interoperabilidad independientemente de la plataforma que se utiliza. En este trabajo se han realizado prácticas de laboratorio utilizando dos sistemas operativos diferentes, Microsoft Windows y Linux Debian, comprobándose de esta manera que a pesar que los sistemas operativos son diferentes, la certificación cruzada (APIs criptográficas, aplicaciones) ha logrado interoperar sin presentarse problemas.

En el ambiente Microsoft Windows se ha utilizado la CA que viene incorporada al sistema operativo y se han generado certificados raíz y subordinados. Así mismo, en el ambiente Linux Debian, se ha utilizado el OpenSSL para la generación de certificados raíz y subordinados. En ambos

sistemas se han utilizado los certificados y han logrado interoperar, confirmándose de esta manera que las funcionalidades mínimas que se requieren para efectuar la certificación cruzada están apegados a un estándar.

Dada la interoperabilidad entre plataformas, las extensiones en los certificados deben cumplir con el estándar antes mencionado, de manera que las aplicaciones puedan reconocer los valores que deben ser validados y aplicados independientemente de la plataforma.

2.4 Elementos requeridos para la implementación de un modelo de certificación cruzada.

Para efectuar la certificación cruzada, se requiere que el certificado de la CA subordinada de la FCE sea firmado por el certificado de la CA subordinada de la FI, esto se logra utilizando la Subordinación Calificada [7] (qualified subordination) permitiendo establecer confianza entre CAs que se encuentran en jerarquías separadas. La certificación cruzada no está limitada a CAs subordinadas, por lo que se pueden establecerse confianza entre una CA raíz y una subordinada, todo dependerá de las necesidades de implementación.

Mediante la Subordinación Calificada, se puede también establecer reglas que permiten validar los certificados que son aceptados entre jerarquías, esto limita los certificados que deben ser válidos para determinada jerarquía. Por ejemplo, la FI requiere que únicamente el certificado de la FCE cuyo asunto refleja el nombre websrv.fce.uba.ar sea aceptado, de esta manera se logra la aplicación del principio del menor privilegio. Lo anterior se logra utilizando la extensión “Name Constraints”.

Las reglas de nombres pueden aplicarse a los siguientes formatos:

- RDN: Identifica los nombres de objetos almacenados en directorios como un LDAP. Ejemplo: DirectoryName = "O = Universidad de Buenos Aires, DC = FCE, DC = UBA, DC = AR".
- DNS: Identifica los nombres de objetos (dispositivos de red, equipos, etc.) en el formato del Sistema de Nombres de Dominio (DNS). Ejemplo: DNS = websrv.fce.uba.ar
- URI: Identifica los nombres de recursos que utilizan el formato Uniform Resource Locator (URL), File Transfer Protocol (FTP) y Hypertext Transfer Protocol (HTTP). Ejemplo: URL = http://websrv.fce.uba.ar
- Correo electrónico: Identifica los nombres utilizando el formato de correo electrónico. Ejemplo: Email = @fce.uba.ar
- UPN: utilizado en la extensión nombre alternativo de asunto (subject alternative name) que puede incluir dominios o direcciones IP.

Adicionalmente se pueden definir los propósitos de aceptación de certificados, esto permite que se puedan establecer políticas de aplicación (Aplication Policies) utilizando los OID de certificados digitales de manera que únicamente los propósitos destinados para cierta aplicación sean válidos. Por ejemplo los OID 1.3.6.1.5.5.7.3.1 para autenticación de servidor, 1.3.6.1.5.5.7.3.2 para autenticación de cliente, 1.3.6.1.5.5.7.3.3 para autenticación de código y 1.3.6.1.5.5.7.3.4 para autenticación en email pueden incluirse en el certificado cruzado para permitir únicamente los certificados de EE que fueron emitidos para estos propósitos.

III Proceso de certificación cruzada

Objetivo de este capítulo: mostrar las tareas del proceso de certificación cruzada que se debe llevar a cabo y mediante la descripción del procedimiento detallar las tareas que se deben llevar a cabo en el sistema operativo Windows server 2008.

Las tareas esenciales del proceso de certificación cruzada consisten en:

- Creación de la plantilla **Cross Certification Enrollment Agent**.
- Incorporación de plantillas **Cross Certification Enrollment Agent** y **Cross Certificate Authority** a la lista de emisión de certificados.
- Emisión del certificado para el Agente **Cross Certification Enrollment Agent**.
- Creación y parametrización del archivo de políticas de certificación (policy.inf).
- Firmado de la solicitud del certificado (req).
- Emisión del certificado cruzado (firmado de la solicitud con la clave privada de la Autoridad Certificante).
- Verificación de las propiedades del certificado cruzado.
- Distribución de la cadena de certificación.

En las siguientes secciones se explica el procedimiento para la creación, configuración y ejecución de tareas que conllevan la creación de un certificado cruzado entre Autoridades Certificantes. El procedimiento se ejecuta en el equipo con la CA Subordinada de la FI (servidor Windows server 2008)

3.1 Creación de la plantilla del Agente para la solicitud de firmado (req)

Con esta plantilla se habilita la emisión de certificados con la característica Qualified Subordination. Esta característica permite incluir en el certificado las políticas o restricciones que se han seleccionado y que deben ser incluidas en el certificado digital cruzado.

Acceda a la consola de administración de la CA, Startup → Administrative tools → Certification Authority. Seleccione **Certificate Templates** utilizando el botón derecho del mouse y posteriormente la opción **Manage.**

En la **Consola de Plantillas de Certificados**, proceda a duplicar la plantilla de **Enrollment Agent.** Seleccione con el botón derecho del mouse esta plantilla y a continuacion la opción **Duplicate Template**.

Se presenta la ventana de advertencia indicando que la plantilla puede ser creada utilizando opciones avanzadas. No todas las Autoridades Certificantes son compatibles con estas propiedades, por lo que para los fines de este laboratorio seleccione Windows 2003 Server, Enterprise Edition.

Se presentan las propiedades relativas a la nueva plantilla. En la opción **Template display name**, coloque un nombre descriptivo en función de las necesidades. (eje. Cross Certification Enrollment Agent).

El establecimiento de los parametros, dependeran de las necesidades en cada situación. En los siguientes pasos se muestran los parametros mínimos que deben establecerse.

Seleccione la viñeta **Extensions** y seguidamente, edite la opción **Applicacion Policies** utilizando el botón **Edit.**

En la ventana **Edit Application Policies Extension**, seleccione la política de aplicación **Certificate Request Agent** y seleccione el botón **Remove.**

Seguidamente seleccione el boton **Add**, agregue la política de aplicación **Qualified Subordination** y seguidamente el botón **OK.**

En la lista políticas de aplicación, únicamente deberá observarse **Qualified Subordination.**

Seleccione el botón **OK** y seguidamente el botón **OK** de la ventana **Propierties of New Template.**

3.2 Incorporación de las plantillas de certificación cruzada a la lista de emisión de certificados

Para poder realizar la emisión de los certificados cruzados, es requerido incoroporar en la lista de plantillas de emision autorizadas a la que fue preparada en la seccion anterior.

En la Consola de la Autoridad Certificante, seleccione **Certificate Templates** utilizando el botón derecho del mouse, seguidamente la opción **New** y posteriormente **Certificate Template to Issue.**

De la lista **Enable Certificates Templates**, localice las plantillas **Cross Certification Authority** y **Cross Certification Enrollment Agent** (Utilice la tecla Ctrl para seleccionar más de una plantilla). Posteriormente presione sobre el botón **OK**.

Asegúrese que las nuevas plantillas aparecen en la lista de **Plantillas de Certificados.**

3.3 Emisión del certificado Cross Certification Enrollment Agent

Para poder emitir el certificado cruzado, se debe seguir el siguiente procedimiento, mismo que debe realizarse en la consola de administración de certificados de la CA Subordinada FI.

En la consola de administración de certificados (certmgr.msc), seleccione la opción **Request New Certificate**. Al iniciar el asistente de Enrolamiento de Certificados, seleccione el botón **Next** hasta llegar a la ventana **Request Certificates.**

Seleccione la casilla **Cross Certification Enrollment Agent** (esta plantilla fue la que se agregó en la sección anterior) y continúe con el asistente.

Asegúrese que la creación del agente se efectuó satisfactoriamente, verificando el **STATUS: Succeeded.**

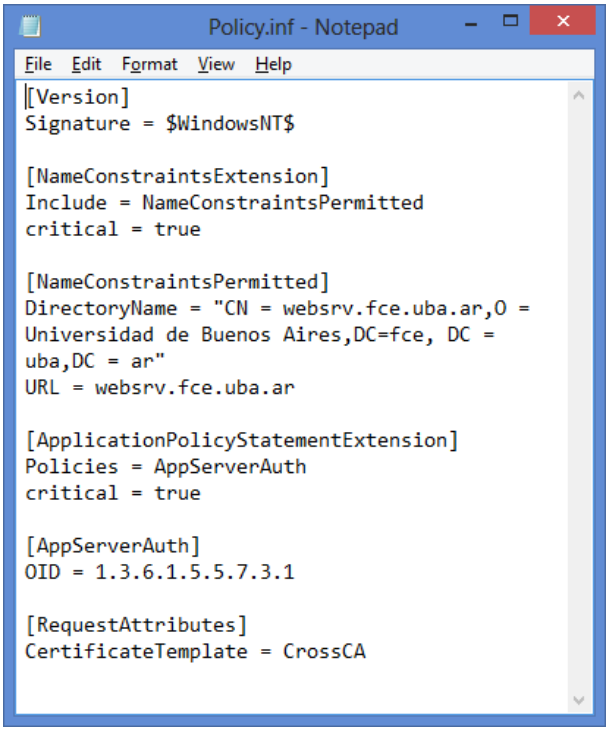
Verifique que el agente se ha agregado a la lista de certificados emitidos y que el propósito corresponda a **Qualified Subordination**. En este caso el usuario **Administrador** es el que tiene el permiso de utilizar este agente.

3.4 Creación y parametrización del archivo de políticas de certificación

El archivo de políticas (policy.inf) está compuesto por secciones que establecen algunos parámetros que determinan el comportamiento del certificado cruzado entre las Autoridades Certificantes.

Este es un archivo de texto cuya ubicación y extensión no es específica, por lo que puede ubicarse en cualquier directorio del servidor y puede tener cualquier extensión, se recomienda que esta última sea **.inf** con el propósito de mantener un estándar en las extensiones de archivos utilizados para la creación de CAs.

Algunos parámetros se utilizan como reglas de nombres o aplicacion para establecer las restricciones que el certificado cruzado valida en los certificados presentados por los servidores. A continuación se muestra un ejemplo.



Cada sección utilizada en el archivo policy.inf se describe a continuación:

Sección/Campo	**Parámetro**	**Descripción**
[Version] Signature=	"$Windows NT$"	Indica el sistema operativo para el cual este archivo es válido. Para la familia de servidores Windows se indica el parámetro.
[NameConstraintsExtension]	Include	Indica las restricciones que se incluyen, si la expresión concuerda, otorga el permiso de uso.
	Exclude	Indica las restricciones que se excluyen, si la expresión concuerda, deniega el permiso de uso.
	Critical [yes/no]	Indica si el parámetro es crítico, si es “yes” aparece el símbolo de un triángulo amarillo.
[BasicConstraintsExtension]	PathLength	Indica el número de niveles de la jerarquía que la certificación cruzada (bajo este nivel) reconocerá como válida.
[ApplicationPolicyStatementExtention]	Policies	Indica los tipos de certificados que serán reconocidos por la Certificación Cruzada.
	Critical [yes/no]	Indica si el parámetro es crítico, si es “yes” aparece el símbolo de un triángulo amarillo.
[RequestAttributes]	CertificateTemplate	Indica el nombre de la plantilla que se usará para firmar la solicitud de Certificación Cruzada

3.5 Firmado de la solicitud del certificado (req)

Mediante la ejecución de la línea de comando **certreq –policy** se genera la solicitud de certificación cruzada, de acuerdo al siguiente procedimiento:

Al ejecutar el comando, proporcione la ubicación del archivo **subca-fce.crt** que contiene el certificado de la **Autoridad Certificante Subordinada** de la FCE. Al seleccionar el botón **Open**, proporcione la ubicación del archivo **policy.inf** (archivo que contiene las reglas de nombres o aplicación correspondientes). Seguidamente seleccione el botón **Open.** El sistema busca la clave privada correspondiente al **Agente de Certificación Cruzada** (Cross Certification Enrollment Agent)**.**

Seleccione el agente correspondiente. Puede seleccionar la opción **Click here to view certificate properties** para ver más detalles del certificado. Asegúrese que el certificado seleccionado tenga como propósito **Qualified Subordination,** seguidamente seleccione el botón **OK.**

Seguidamente se solicita un nombre para el archivo de solicitud que se ha firmado con la clave privada del Agente de Certificación Cruzada, utilice el nombre **fce-subca-request.req**. Al seleccionar el botón **Save**, el archivo está listo para ser enviado a la Autoridad Certificante Integrada de la FI para ser firmado con la clave privada de ésta CA.

3.6 Emisión del Certificado Cruzado

Ingrese a la consola de la Autoridad Certificante Integrada (puede utilizar el comando certsrv.msc), seleccione con el botón derecho del mouse sobre el identificador que corresponde a la Autoridad Certificadora (Autoridad Certificante Integrada Laboratorio PSI), seleccione **All Tasks** y seguidamente **Submit new request…**

Proporcione el archivo que corresponde a la solicitud firmada por el **Agente de Certificación Cruzada** (archivo **fce-subca-request.req**) y presione el botón **Open.**

Esto permite firmar con la clave privada de la AC Subordinada FI la solicitud y se obtiene el **Certificado Cruzado**, seguidamente solicita la ubicación para almacenarlo**.** Utilice el nombre **fce-subca-cross-sign.cer**

3.7 Verificación de las propiedades del certificado cruzado

El archivo se almacena con extensión **.cer**. Al ejecutar este archivo, se muestran las propiedades del **Certificado Cruzado**, en la viñeta **General** se muestran las propiedades del certificado junto con los propósitos para los cuales el certificado ha sido emitido, a quien se ha emitido (FCE SubCA), quien lo emitió (Autoridad Certificante Integrada Laboratorio PSI de la FI) y las fechas de validez.

En la viñeta **Details**, se muestran el valor del **Subject Key Identifier** que corresponde al certificado de la **Autoridad Certificante Subordinada de FCE** y el **Authority Key Identifier** debe corresponder a la **Autoridad Certificante Integrada FI**.

La viñeta **Certification Path** presenta la cadena de certificación, donde se muestra la jerarquía que corresponde a la FI.

3.8 Distribución de la cadena de certificación

La utilización del Certificado Cruzado, requiere una distribución adecuada de la cadena de certificación. En infraestructuras con Windows que tienen una numerosa cantidad de estaciones de trabajo, esta cadena puede ser distribuida por medio del **Group Policy**. Esta utilidad permite almacenar el certificado cruzado en el repositorio de Autoridades Certificantes Intermedias de confianza.

El siguiente procedimiento se debe efectuar en todos los equipos que van a interactuar con el servidor web de FCE (Servidor Linux Debian con Apache). Instale el certificado cruzado en el almacén de **Autoridades Certificantes Intermedias** de la **Autoridad Certificante Integrada Laboratorio PSI** de la FI.

Seleccione el botón **Install** que se encuentra en la viñeta **General** de las propiedades del certificado.

Se inicia el asistente para importar certificados, seleccione el botón **Next** y en la siguiente ventana seleccione la opción **Place all certificates in the following store** seguidamente el botón **Browse.**

Seleccione el almacén denominado **Intermediate Certification Authorities** y a continuación el botón **OK.**

Finalice el asistente seleccionando el botón **Next** y **Finish** asegúrese de que aparezca la ventana de confirmación que indica que el certificado fue importado satisfactoriamente.

Compruebe que tiene acceso a la url **https://websrv.fce.uba.ar** y que no se presenta ninguna alerta de error de certificados.

3.9 Consideraciones que se deben tomar en cuenta al momento de implementar este modelo

Para la implementación de este modelo, es recomendable que se tomen en cuentas las siguientes consideraciones:

- Debe existir el principio de emisión de subjects únicos, es decir no deben emitirse dos certificados con el mismo nombre y que estén activos al mismo tiempo. Por lo que debe revisarse que la organización que emite los EE tenga incluido este principio en sus políticas.

- Definir los propósitos del certificado cruzado de manera que coincida con las actividades para los cuales fue destinados (aceptar certificado de servidor, cliente, email, etc).

- Se debe distribuir el certificado cruzado en el almacén de certificados intermedios de confianza en los equipos de los usuarios que acceden los recursos de la otra organización.

- Debido a que el certificado cruzado pasa a ser subordinado de la organización, se debe prestar atención especial que de revocarse este certificado, aparecerá en la CRL de esta misma organización y no en la otra. En nuestro escenario, aparecerá en la CRL de la FI.

3.10 Procedimiento para la gestión de los certificados digitales que se han cruzado.

Los procedimientos para la gestión de certificados digitales, deben ser adecuadamente documentados y los interesados deben seguir éste con el propósito de evitar en la medida de lo posible cualquier incidente de seguridad.

Los procedimientos para la gestión de certificados digitales cruzados deben adecuarse a cada situación organizacional, por lo que se recomienda seguir un ciclo como el descrito a continuación para una adecuada gestión.

Thales e-security propone un modelo relacionado con el ciclo de vida de las claves [8] desde la generación hasta la destrucción. Este modelo permite una administración sistemática de las claves en general y puede ser utilizado en certificados digitales cruzados. El modelo consiste en:

- Generación: Proceso por el cual una nueva clave se genera.
- Registro: Proceso por el cual una clave es asociada a un usuario, aplicación o servicio.
- Almacenamiento: Proceso por el cual la clave es almacenada en un lugar seguro o inaccesible por entes no autorizados.
- Respaldo y restauración: Proceso por el cual la clave debe ser respaldada para evitar que en un desastre ésta se pierda afectando las operaciones del negocio.
- Distribución/Instalación: Proceso por el cual una clave se distribuye o se instala para su posterior uso. Este proceso debe estar acompañado de una validación apropiada del ente que va utilizar la clave al momento de la entrega.
- Uso: Proceso por el cual la clave es utilizada

    - Rotación: Proceso por el cual la clave se redefine o se rota de acuerdo a una política de riesgo, evitando una ventana muy amplia de ataque por uso prolongado.
    - Revocación: Proceso por el cual la clave se revoca debido a un incidente.
- Suspensión: Proceso por el cual se determina que la clave ha culminado su vida operacional y debe ser reemplazada.
- Destrucción: Proceso por el cual la clave es destruida si no se requiere más su existencia.

Los certificados cruzados deben ser manejados con extremo cuidado, ya que estos permiten o limitan el acceso a determinados servicios o aplicaciones. Para que un certificado cruzado preste los servicios adecuadamente, las aplicaciones o servicios deben ser capaces de determinar la validez de la cadena de certificación que emitió el certificado. Los sistemas operativos incluyen APIs criptográficas que acceden al almacén de certificados de confianza y verifican el hash del certificado cruzado (o cualquier certificado) que ha sido cifrado utilizando la clave privada de la CA subordinada (o cualquier CA de la jerarquía). Esta verificación se hace descifrando el hash por medio de la clave pública de la CA subordinada (quien es la única que puede descifrar lo que la clave privada cifro) verificando la validez de los certificados.

Dicho lo anterior, es importante que el almacén de certificados de confianza sea protegido para evitar que se guarden certificados cruzados (y cualquier otro en general) que ponga en riesgo el proceso de comprobación.

3.11 Mejores prácticas para la gestión de certificados digitales cruzados

Al planificar las condiciones para la certificación cruzada, se deben seguir las siguientes prácticas [9]:

- Definir únicamente las condiciones requeridas.
- Excluir el espacio de nombres en todas las restricciones de quien va a efectuar el proceso de certificación cruzada.
- Involucrar al departamento legal en las negociaciones que compete la relación de negocios
- Crear una Autoridad Certificante de Certificados cruzados para emitir certificados separados para cada proyecto.
- Emitir los certificados cruzados permitiendo únicamente los propósitos destinados (Application policy), es decir si es para autenticar firma de código solo debe permitirse el OID 1.3.6.1.5.5.7.3.3 **(**Code Signing).

3.12 Prueba de concepto de la solución

En el anexo se encuentran los laboratorios que permitieron llevar a cabo la prueba de concepto de la solución. Para esta prueba se determinó utilizar diferentes sistemas operativos para la generación de la CAs con el propósito de verificar la interoperabilidad de los certificados digitales emitidos.

La prueba de concepto se desarrolló considerando un escenario entre dos organizaciones, la Facultad de Ingeniería y la de Ciencias Económicas. En el ambiente Windows de la FI se tienen dos instalaciones, una de ellas tiene una CA Raíz y la otra una CA subordinada, esta última está integrada además al servicio Active Directory Domain Services (ADDS) en la misma instalación. En el ambiente Linux Debian OpenSSL se tiene una sola instalación con un CA Raíz y una Subordinada.

Las CAs subordinadas han sido designadas para emitir certificados para EE y en este mismo nivel se ha efectuado la certificación cruzada, es decir, el certificado de la CA FCE subordinada es enviado a la CA FI para que esta última lo firme y forme parte de la jerarquía de la FI. Al instalar el certificado cruzado en los equipos de la FI, las APIs criptográficas del sistema operativo reconocen los certificados que han sido emitidos por la CA Subordinada de la FCE, por lo que no es requerido que los certificados de las CAs Raíz y Subordinada (pertenecientes a las CAs de la FCE) sea instalados en los equipos de la FI.

En relación a las restricciones (constraint), al efectuar el proceso de certificación cruzada, el archivo (policy.inf) que contiene las políticas establece los parámetros (definidos por las organizaciones) que permiten o deniegan los certificados que serán reconocidos.

En la sección NameConstraintsExtension del archivo policy.inf, se hace referencia a las expresiones que incluyen (Include) y que excluyen (Exclude) un criterio de aceptación del certificado. Para la prueba de concepto se utiliza una expresión que solamente permite un certificado digital cuyo subject sea **websrv.fce.uba.ar** de esta manera cualquier otro certificado que no tenga este nombre debe ser rechazado. Es importante mencionar que dentro de las políticas de emisión de certificados (funciones administrativas de la PKI) debe existir el principio de emisión de subjects únicos, es decir no deben emitirse dos certificados con el mismo nombre y que estén activos al mismo tiempo.

3.13 Problemas encontrados en el proceso

Al efectuar el proceso de certificación cruzada se encontraron algunos problemas:

- No existe una plantilla que corresponda al firmado de la solicitud del certificado cruzado por lo que hay que crearla anteriormente. Sección 3.1

- La cadena de certificación debe ser distribuida en los equipos de la FI que van a acceder a los recursos de la FCE. Es de hacer notar que en ningún momento se requiere que los certificados raíz y subordinada no deben instalarse en éstos mismo equipos. Sección 3.8
- El tiempo de duración de la plantilla Cross Certification Authority no debe ser mayor a la del certificado de la CA que se prentende firmar. En el caso de Windows, esta plantilla viene definida por defecto.

Conclusiones

En este documento vimos que el modelo de certificación cruzada permite a organizaciones autónomas establecer un modelo de confianza mutua en forma simple y escalable. Hoy en día las organizaciones ya tienen definida una jerarquía de CAs, a partir de la cual se pueden definir el o los puntos de confianza a cualquier nivel con respecto a la otra jerarquía.

Esta característica es particularmente práctica, desde el punto de vista de seguridad, debido a que se pueden establecer reglas de restricción para limitar los nombres o aplicaciones de los certificados de la otra organización que se han de aceptar.

Es particularmente importante recalcar que en el establecimiento de la confianza no se tiene que crear una CA común entre las organizaciones, evitando la duplicidad de recursos y facilitando la administración. Una opción utilizada en estos casos es que la CA común sea la raíz de ambas jerarquías eso llevaría a que los certificados emitidos se deban revocar y volver a emitir.

En el modelo de certificación cruzada, el establecimiento de la confianza se realiza intercambiando las certificaciones de las CA de cada organización, de esta forma simplificando el despliegue del sistema.

Mediante la prueba de concepto, se ha demostrado y validado que la certificación cruzada proporciona un buen modelo de confianza y permite la interoperabilidad de certificados digitales entre distintas plataformas típicamente presentes en organizaciones grandes. Para ello se proponen configuraciones y políticas de trabajo que permiten su despliegue en ambientes heterogéneos Windows/Unix.

Este modelo es muy recomendable, en instituciones de banca central destinadas a la administración y control del Sistema Financiero (bancos,

financieras, casas de cambio, etc.) debido a la interacción que éstas últimas tienen con el banco central. De esta manera, las aplicaciones que los bancos centrales ponen a disposición de sus asociados pueden establecer un punto de confianza sin verse en la necesidad de redefinir su ambiente de PKI o el de los asociados.

Es mi objetivo profundizar esta investigación para resolver la problemática del sistema financiero el cual es de mucho interés para mi dado que la organización para la cual desempeño mis actividades laborales es el Banco Central de Honduras. Entiendo que este modelo podrá ser muy útil para resolver la problemática de confianza con los asociados.

Glosario [10]

Activo	(Inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización.
Amenaza	(Inglés: Threat). Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
Autenticación	(Inglés: Authentication). Segú [Magerit:1997]: Característica de dar y reconocer la autenticidad de los activos del dominio (de tipo información) y/o la identidad de los actores y/o la autorización por parte de los autorizadores, así como la verificación de dichas tres cuestiones..
Autenticidad	(Inglés: Authenticity). Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
Autoridad de Registro	Ente de validación de la identidad y otros datos de los suscriptores de certificados.
Confidencialidad	(Inglés: Confidenciality). Acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.
Control	Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

Disponibilidad	(Inglés: Availability). Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.
Gestión de claves	(Inglés: Key management). Controles referidos a la gestión de claves criptográficas.
Incidente	Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Integridad	(Inglés: Integrity). Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.
Interoperabilidad de certificados	La operación valida entre certificados emitidos por distintas plataformas.
No repudio	Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).
Prueba de Concepto	Una prueba de concepto o PoC (por sus siglas en inglés) es una implementación, a menudo resumida o incompleto, de un método o de una idea, realizada con el propósito de verificar que el concepto o teoría en cuestión es susceptible de ser explotada de una manera útil

Riesgo	(Inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.
Trazabilidad	(Inglés: Accountability). Según [CESID:1997]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Bibliografía Específica

[1] K. Raina, PKI Security Solutions for the Enterprise, Indianapolis, Indiana: Wiley Publishing, Inc., 2003.

[2] R. A. Española, «Diccionario de la lengua española,» Real Academia Española, [En línea]. Available: http://www.rae.es/rae.html, http://www.rae.es/drae/srv/search?id=ttIyhpiT7DXX2p26VbYf. [Último acceso: 7 6 2013].

[3] DATALOSSdb, «DATALOSSdb,» Open Security Foundation, 21 06 2013. [En línea]. Available: http://datalossdb.org/incidents/10397-6-million-users-email-addresses-and-phone-numbers-exposed-due-to-a-bug. [Último acceso: 29 06 2013].

[4] Certisur, «Certisur,» [En línea]. Available: https://www.certisur.com/eventos-y-noticias/201207-Nuevas-Normativas.

[5] Certification Authority Browser Forum, «CA/Browser Forum,» CA/Browser Forum, [En línea]. Available: https://www.cabforum.org/forum.html. [Último acceso: 13 07 2013].

[6] R. Kuhn, V. C. Hu, T. Polk y S.-J. Chang, Introduction to Public Key Technology and the Federal PKI Infrastructure SP 800-32, National Institute of Standards and Technology, 2001, p. 15.

[7] Microsoft Corpotation, «Qualified subordination overview,» Microsoft Corpotation, 2005 Enero 2005. [En línea]. Available: http://technet.microsoft.com/en-us/library/cc786077(v=ws.10).aspx. [Último acceso: 14 07 2013].

[8] R. Moulds, Key Management For Dummies, Hoboken: Wiley, 2001.

[9] B. Komar, Windows Server 2008 PKI and Certificate Security, Redmond, Washington: Microsoft Press, 2008.

[10] E. p. d. l. 27001, «El portal de ISO 27001,» [En línea]. Available: http://www.iso27000.es/glosario.html. [Último acceso: 09 10 2013].

[11] G. Millan, «Infraestructuras de certificacion cruzada,» *Boletin de RedIRIS,* vol. 71, nº Enero http://www.rediris.es/difusion/publicaciones/boletin/70-71/ponencia14.pdf, enero 2005.

[12] «OpenSSL PKI Tutorial,» [En línea]. Available: http://pki-tutorial.readthedocs.org/en/latest/simple/index.html. [Último acceso: 26 10 2012].

[13] «Debian Project,» [En línea]. Available: http://www.debian.org/.

[14] «Open SSL Project,» [En línea]. Available: http://www.openssl.org/.

[15] B. Komar, Windows Server 2008 PKI and Certificate Security, Microsoft Press, 2008.

[16] «Trust Models,» Microsoft Corporation, [En línea]. Available: http://msdn.microsoft.com/en-us/library/windows/desktop/bb540815(v=vs.85).aspx. [Último acceso: 26 10 2012].

[17] «Certificate Hierarchy,» Microsoft Corporation, [En línea]. Available: http://msdn.microsoft.com/en-us/library/windows/desktop/bb931353(v=vs.85).aspx. [Último acceso: 26 10 2012].

[18] «Certificate Chain,» Microsoft Corporation, [En línea]. Available: http://msdn.microsoft.com/en-us/library/windows/desktop/bb540794(v=vs.85).aspx.

[19] «Cross Certification,» Microsoft Corporation, [En línea]. Available: http://msdn.microsoft.com/en-us/library/windows/desktop/bb540800(v=vs.85).aspx.

[20] Microsoft Corporation, «Developer Network,» Microsoft Corporation, [En línea]. Available: http://msdn.microsoft.com/en-us/library/ms524668(v=vs.90).aspx. [Último acceso: 15 06 2013].

Bibliografía General

[1] K. Raina, PKI Security Solutions for the Enterprise, Indianapolis, Indiana: Wiley Publishing, Inc., 2003.

[2] R. A. Española, «Diccionario de la lengua española,» Real Academia Española, [En línea]. Available: http://www.rae.es/rae.html, http://www.rae.es/drae/srv/search?id=ttIyhpiT7DXX2p26VbYf. [Último acceso: 7 6 2013].

[3] DATALOSSdb, «DATALOSSdb,» Open Security Foundation, 21 06 2013. [En línea]. Available: http://datalossdb.org/incidents/10397-6-million-users-email-addresses-and-phone-numbers-exposed-due-to-a-bug. [Último acceso: 29 06 2013].

[4] R. Kuhn, V. C. Hu, T. Polk y S.-J. Chang, Introduction to Public Key Technology and the Federal PKI Infrastructure SP 800-32, National Institute of Standards and Technology, 2001, p. 15.

[5] R. Moulds, Key Management For Dummies, Hoboken: Wiley, 2001.

[6] B. Komar, Windows Server 2008 PKI and Certificate Security, Redmond, Washington: Microsoft Press, 2008.

Anexos

Laboratorio 1: Creación de una autoridad certificante (CA) subordinada integrada con Active Directory Domain Services (ADDS).

Objetivo

Crear con el Sistema Operativo Windows una autoridad certificante subordinada integrada con ADDS que se utilizará para continuar la cadena de confianza de una organización. Esta CA proporciona además el servicio de emisión de certificados para entidades (usuarios, equipos, etc) finales.

Autoridad Certificante Subordinada Integrada

Una autoridad certificante Subordinada integrada con ADDS, permite emitir certificados de acuerdo a las necesidades de una organización, por ejemplo, si la organización requiere que los usuarios utilicen certificados para efectuar el proceso de autenticación o certificados para autenticar los dispositivos que se conectan a la red.

La autoridad certificante integrada con ADDS, es un servidor que debe mantenerse encendido y operacional para poder ofrecer el servicio de generación de certificados.

Nota: Este servidor debe generar una lista de revocación de certificados (CRL) en lapsos de tiempo coherentes a las necesidades del negocio. A diferencia de la CA raíz y subordinada que los tiempos de generación CRL son relativamente más largos. Los certificados de los usuarios finales están expuestos a una mayor cantidad de amenazas por lo que los tiempos de generación de la CRL deben ser cortos. Así mismo esta CRL debe poder ser accedida desde todos los equipos que tienen las aplicaciones y servicios de la organización, por lo que se debe disponer de un servidor web para

almacenar y publicar este archivo. En estos laboratorios se utiliza la URL http://websrv.fi.uba.ar/publico.

Proceso de creación de la autoridad certificante subordinada integrada con ADDS en Windows server 2008

Para este proceso se utilizara una máquina virtual que contiene Windows server 2008 R2 Enterprise Edition X64.

1. Inicie la Máquina Virtual ***Windows Server 2008 R2 x64 Ent Edition ADDSCS***.
2. Asigne el nombre correspondiente **srvaddscs**.
3. Reinicie la máquina virtual.
4. Promueva este servidor a controlador de dominio mediante el comando ***dcpromo*** El dominio debe ser nombrado: ***fi.uba.ar*** al finalizar el asistente para creación del controlador de dominio, el servidor debe ser reiniciado.

   Nota: Este laboratorio no incluye el procedimiento a seguir para promover un servidor a controlador de dominio.

5. Para comprobar que el servidor ha sido promovido correctamente, en ***Administrative tools*** seleccione la consola de administración de usuarios ***Active Directory Users and Computers*** y verifique que el equipo ***srvaddscs*** se encuentra en la unidad organizativa ***Domain Controllers.***

6. Continúe con este paso una vez que el servidor se ha promovido a controlador de dominio. Mediante la herramienta Initial Configuration Task, seleccione la opción ***Add Roles*** y seguidamente la opción ***Next***.

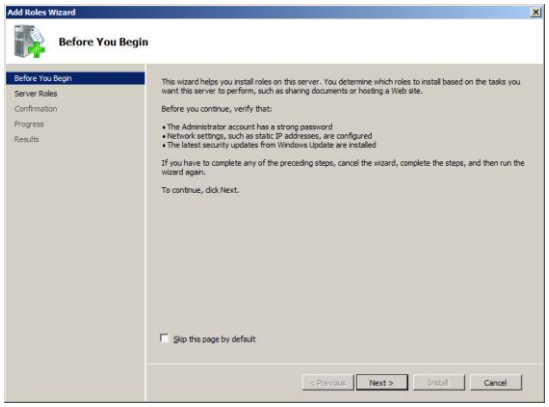


Figura 1. Asistente para agregar roles.

7. Marque la casilla ***Active Directory Certificates Services*** y seleccione el botón ***Next.***

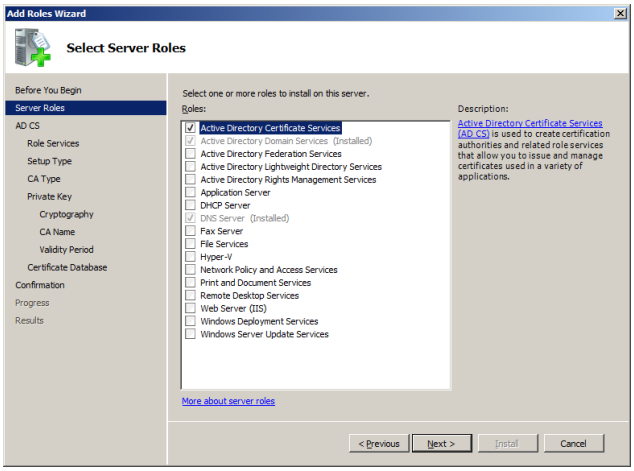


Figura 2. Selección de la casilla ***Active Directory Certificates Services.***

8. Se muestra la ventana que presenta una introducción a los Servicios de Certificados de Active Directory. Seleccione el botón ***Next.***

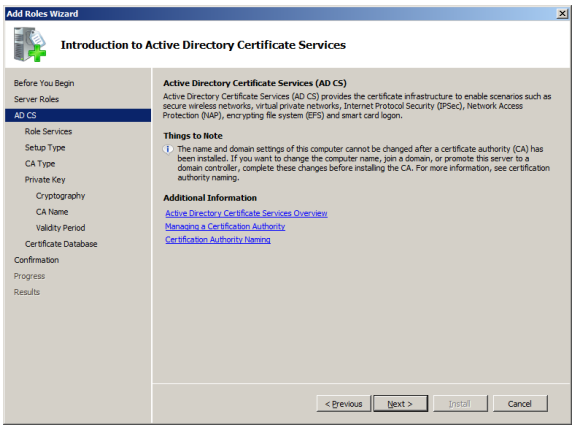


Figura 3. Introducción a los Servicios de Certificados

9. Debido a que esta es una autoridad certificante operativa (emitirá certificados para usuarios finales), se requieren lo servicios ***Certification Authority Web Enrollment y Online responder***, marque las opciones antes indicadas y seleccione el botón ***Next***.

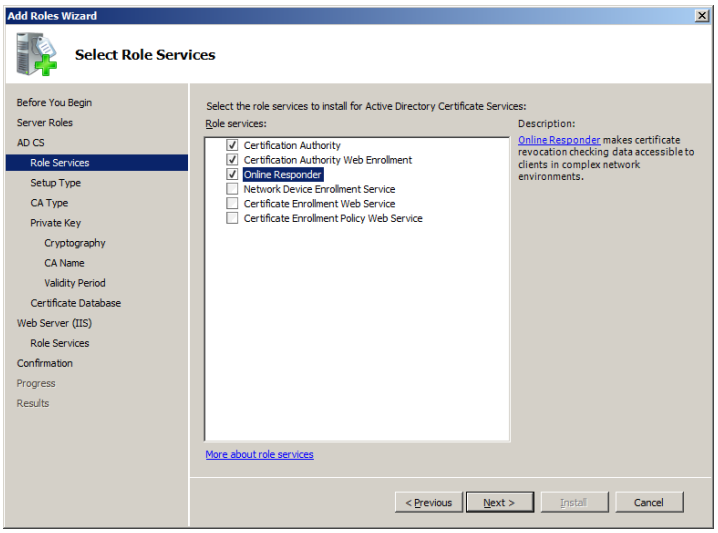


Figura 4. Ventana de selección de roles

Un mensaje informa que se requieren algunos roles y servicios para habilitar la emisión de certificados. Presione el botón ***Add Requiered Role Services.***

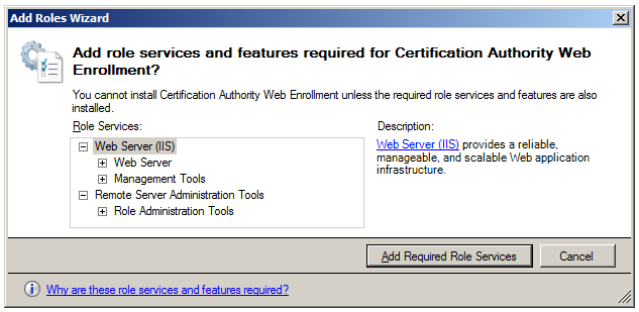


Figura 5. Asistente para agregar roles.

10. Al integrar una CA operativa a un dominio de Microsoft, la siguiente ventana presenta la opción ***Enterprise y Standalone***. Seleccione la opción ***Enterprise*** para integrar la CA al dominio de Microsoft. Seleccione el botón ***Next.***

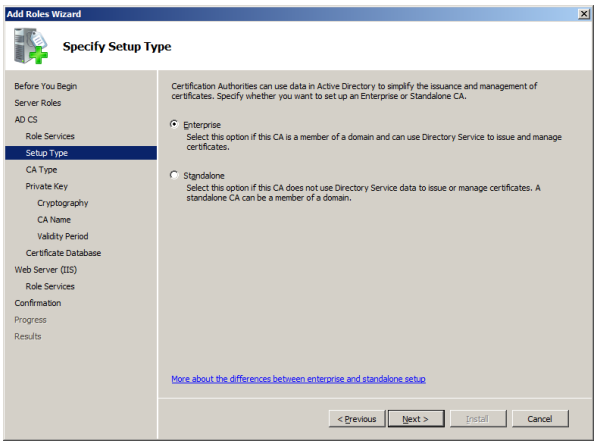


Figura 6. Tipo de configuración

11. Es la siguiente ventana, seleccione la opción ***Subordinate CA*** y seguidamente el botón ***Next.***

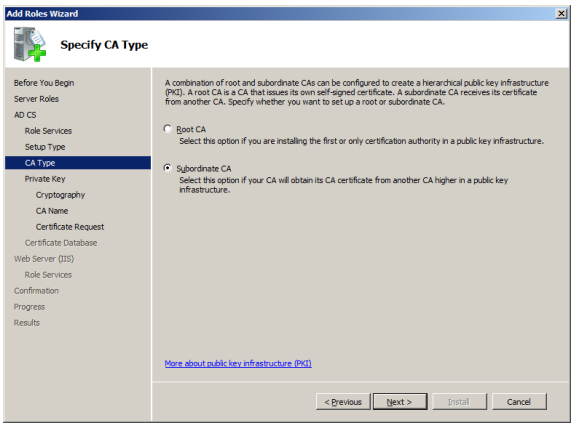


Figura 7. Selección del tipo de autoridad certificante.

12. Seguidamente se presenta la ventana para la creación de la llave privada de la autoridad certificante. Cuando se tiene una llave privada existente, se selecciona la opción ***Use existing private key*** de lo contrario se selecciona la opción ***Create a new private key.***

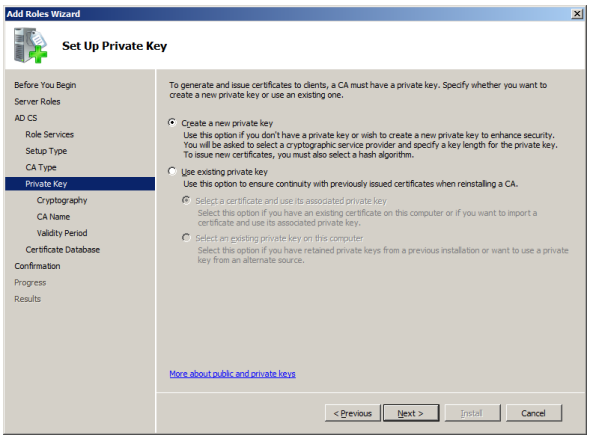


Figura 8. Configuración de la llave privada

13. La ventana siguiente muestra los Cryptography Service Providers (CSP) disponibles para la generación de la llave privada. En la siguiente URL se provee información adicional relacionada con el CSP RSA Microsoft Software Key Storage Provider http://msdn.microsoft.com/en-us/library/windows/desktop/bb931355(v=vs.85).aspx. Este CSP almacena la llave privada en el sistema operativo, para elevar el nivel de seguridad que se requiere para tener un mayor control de uso de la llave privada, se recomienda el uso de dispositivos Hardware

Security Module (HSM) que generan y almacenan la llave privada mediante hardware lo que hace imposible su uso sin la autorización requerida. Un ejemplo de HSM para este fin es el SPYRUS LYNKS Series II.

Para este laboratorio seleccione el CSP RSA #Microsoft Software Key Storage Provider y como algoritmo de Hash SHA1. El Key Character Lenght a 2048. Seguidamente seleccione el botón ***Next***.

Nota: Cuando se utiliza un HSM, es requerido que se marque la casilla ***Allow Administrator Integration when the private key is accessed by the CA.***

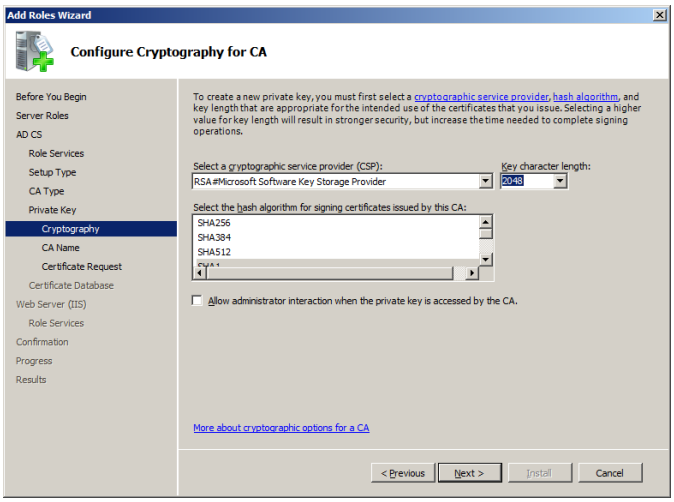


Figura 9. Selección del CSP

14. En la siguiente ventana coloque la dirección LDAP correspondiente y seleccione el botón ***Next***. Debido a que esta CA estará conectada a la red, los valores de esta ruta, deben corresponder al dominio al que pertenece la CA. Utilice los siguientes datos:

Nota: El símbolo al final G# indica el número de grupo, eje. G4

Common name for this CA: ***Autoridad Certificante Integrada Laboratorio PSI G#***

Distinguished name suffix: ***DC=FI,DC=UBA,DC=AR***

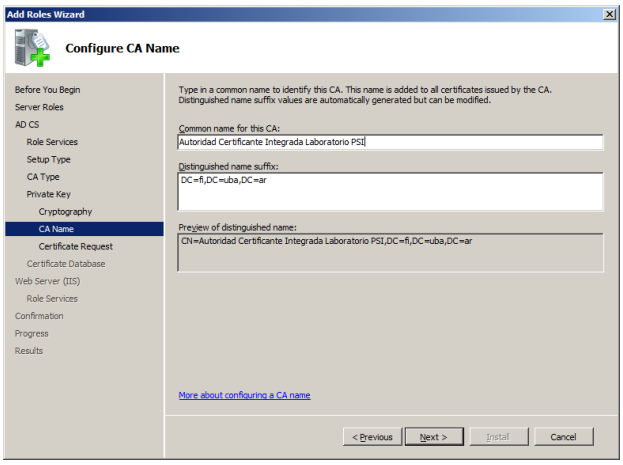


Figura 10. Nombre de la CA Operativa

15. Seguidamente almacene el Certificate Signing Request (CSR) en la ruta predeterminada. Este archivo se debe llevar a la CA raíz para ser firmado con la llave privada.

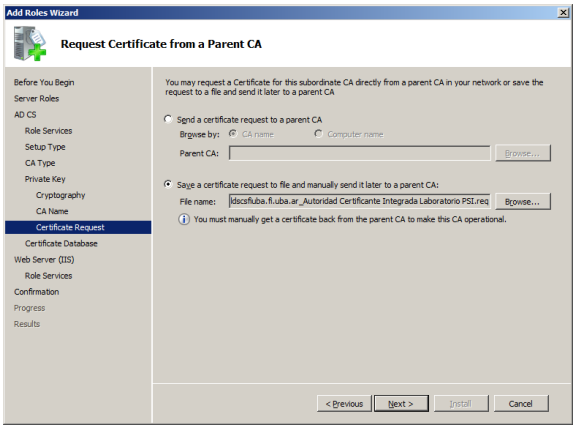


Figura 11. Almacenamiento del Certificate Signing Request (CSR)

16. Seguidamente se muestra la ventana correspondiente a la ubicación de la base de datos de los certificados y logs. Seleccione el botón ***Next.***

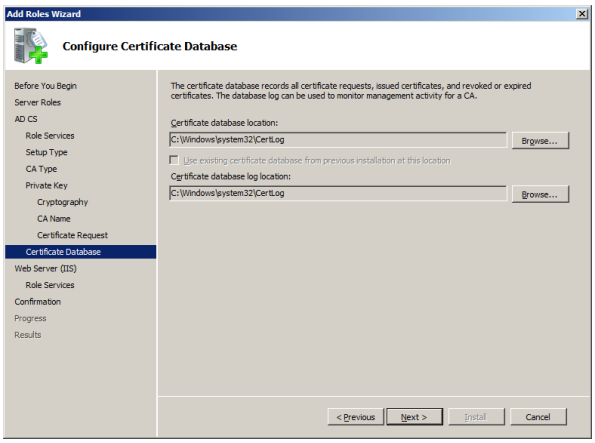


Figura 12. Ubicación de la base de datos de certificados y logs

17. En la siguiente ventana se muestra un mensaje indicando los usos que puede darse al servicio IIS. Presione el botón ***Next.***

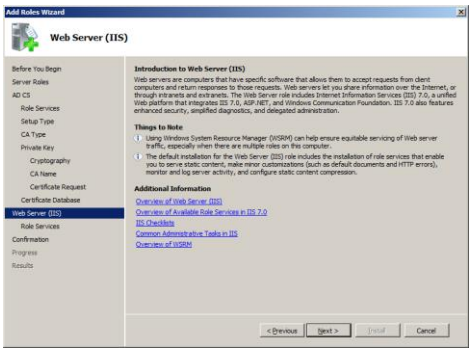


Figura 13. Introducción al servidor IIS

18. A continuación se muestra un resumen de los roles de servicios que serán instalados. Presione el botón ***Next***.

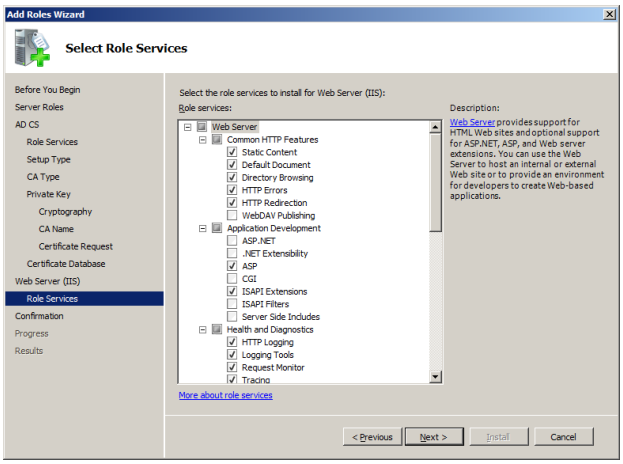


Figura 14. Roles del servicio IIS.

19. Finalmente aparece la ventana presentando un resumen de algunos roles seleccionados en los pasos anteriores. Seleccione el botón ***Install.***

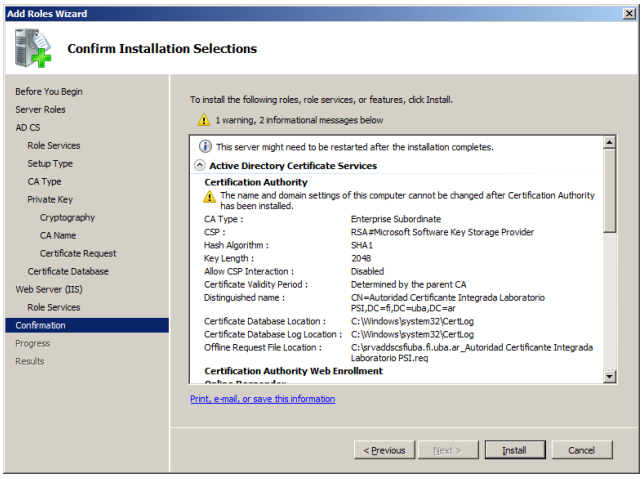


Figura 15. Resumen de Roles seleccionados.

20. A continuación se observa la ventana que presenta el progreso de la instalación.

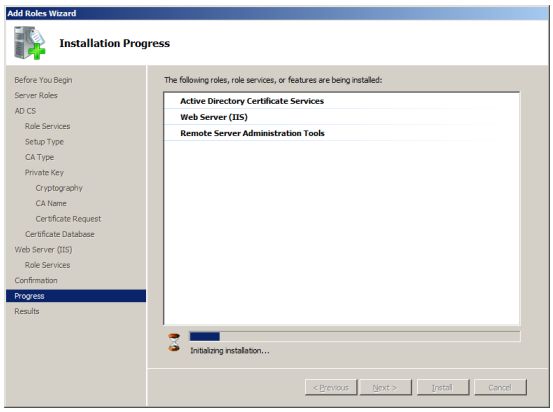


Figura 16. Progreso de instalación.

21. Seguidamente se presenta la advertencia que indica que la instalación no está completa sino hasta que se firme el certificado utilizando la CA raíz. Seleccione el botón ***Close.***

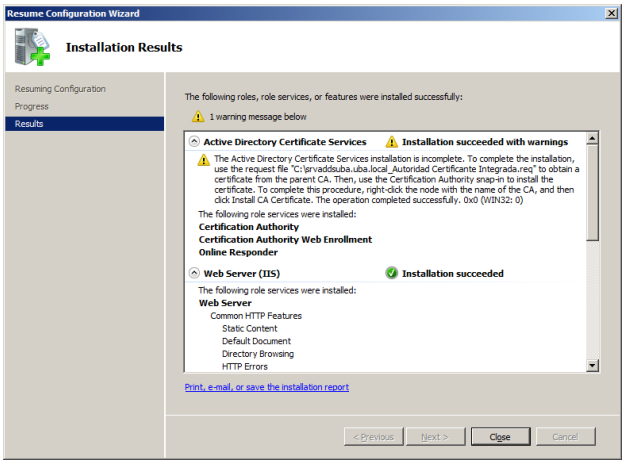


Figura 17. Resultado de la instalación.

Proceso de firmado de la CA integrada

Los siguientes pasos se efectúan en el CA Raíz:

1. Inicie la máquina virtual denominada ***Windows Server 2008 R2 x64 Ent Edition CA Raiz.***

2. Copie en el escritorio de la CA raíz el archivo (archivo .req) que se almaceno en el paso 15 del procedimiento anterior.

3. Inicie la consola de administración de la CA seleccionando ***Inicio → Administration tools → Certification Authority***

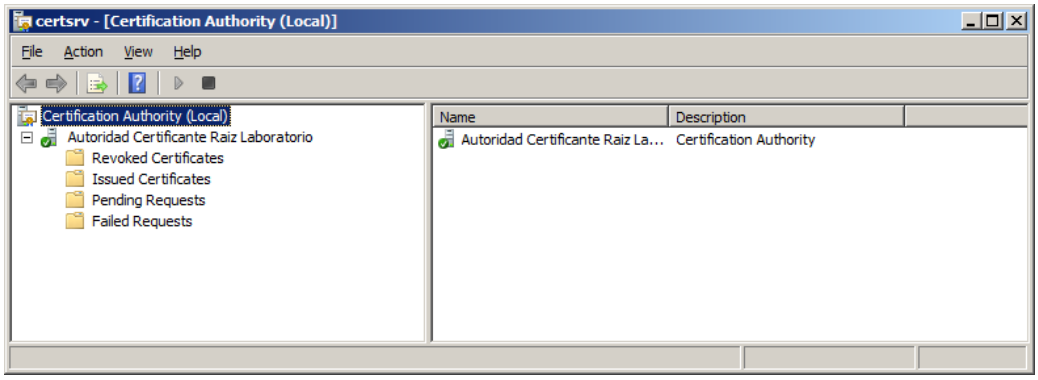


Figura 18. Consola de administración de la CA.

4. Seleccione con el botón derecho del mouse ***Autoridad Certificante Raiz Laboratorio*** seguidamente ***All Task → Submit new request…***

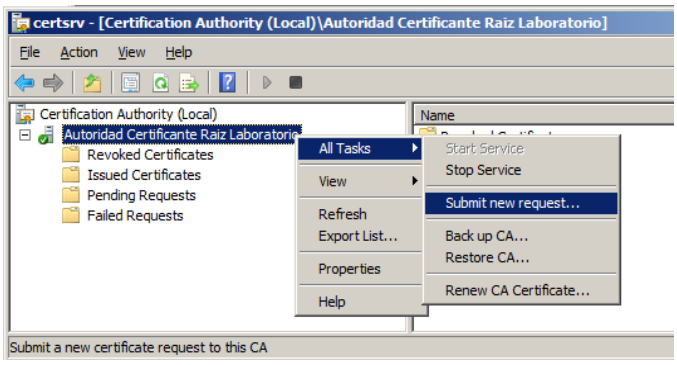


Figura 19. Envío de una nueva solicitud

5. Proporcione el archivo con la solicitud del CA integrada ADDS (Archivo .req que se copió al escritorio).

6. Seleccione la opción ***Pending Requests*** para visualizar las solicitudes pendientes

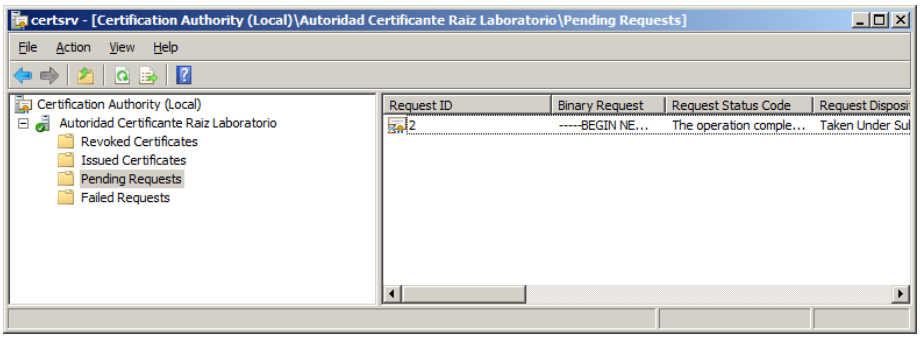


Figura 20. Examinar las solicitudes pendientes

7. Presionando con el botón derecho del mouse seleccione el certificado pendiente de emisión, seguidamente ***All Task → Issue.***

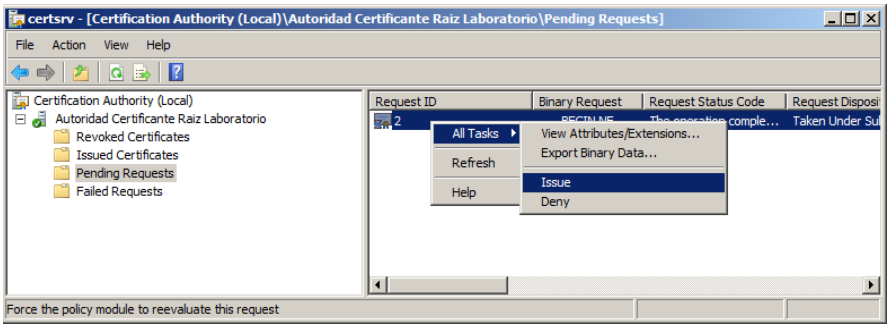


Figura 21. Emisión del certificado del CA Integrada

8. Para verificar la correcta emisión del certificado, seleccione ***Issued Certificates,*** el certificado aparece en la ventana de detalles, con el botón derecho del mouse, seleccione el certificado emitido y a continuación ***Open.***

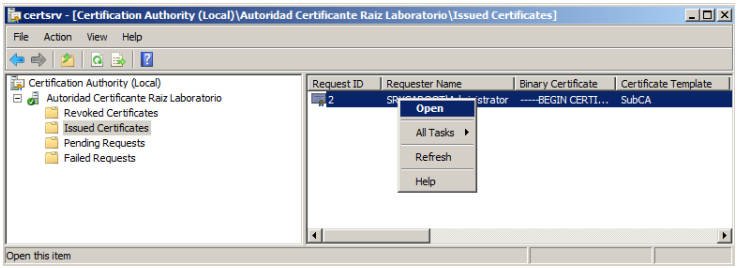


Figura 22. Verificación de la emisión del certificado

9. Verifique que los detalles del certificado corresponden a los que se proporcionaron al momento de configurar la CA Integrada.

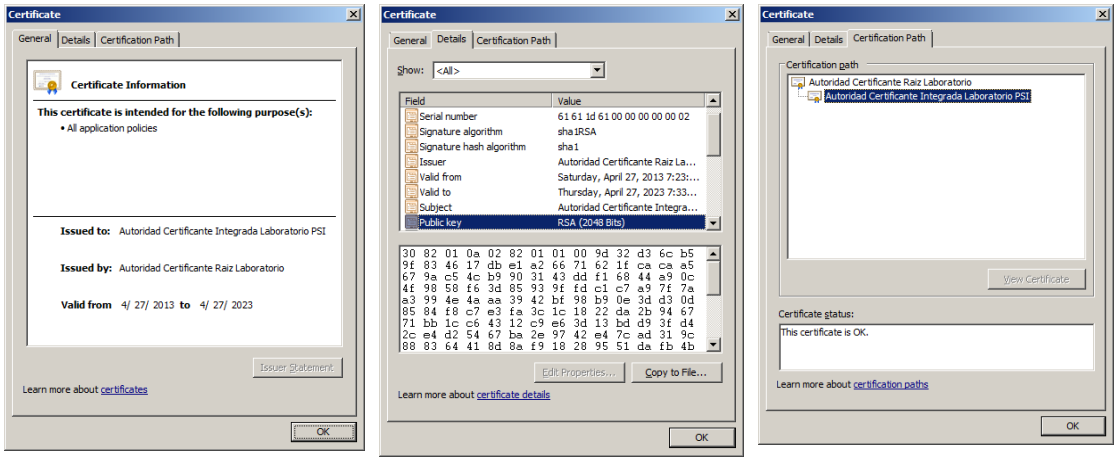


Figura 23. Propiedades del certificado ***Autoridad Certificante Integrada***

10. En la viñeta de detalles, seleccione el botón ***Copy to File...***

11. Se inicia el asistente para la exportación de certificados digitales, seleccione el boton ***Next.*** Para el formato de exportación, seleccione ***Cryptographic Message Sintax Standard – PKCS #7 Certificates (.P7B)*** y marque la casilla ***Include all certificates in the certification path if possible*** y a continuación el botón ***Next***. Asigne una ubicación y un nombre al archivo. Continúe hasta finalizar el asistente.

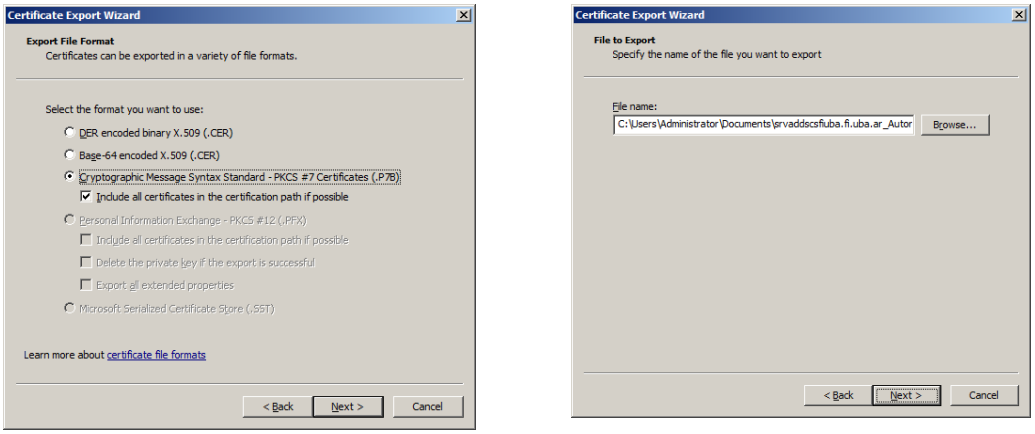


Figura 24. Asistente para la exportación de certificados.

12. Copie el archivo que contiene el certificado firmado por la CA raíz (archivo .p7b del paso anterior) al escritorio del servidor que contiene la CA Integrada.

13. Copie en el escritorio del servidor que contiene la CA Integrada los archivos que se encuentran ubicados en C:\Windows\System32\CertSrv\CertEnroll de la ***Autoridad Certificante Raiz Laboratorio***:

    Ejem.:

    Autoridad Certificante Raiz Laboratorio.crl

    srvrootcafiuba_Autoridad Certificante Raiz Laboratorio.crt

Los siguientes pasos se efectúan en la CA Integrada:

1. Para facilitar la ejecución de comandos posteriores, renombre los archivos del paso 13. a ***carootfiuba.crl*** y ***carootfiuba.crt*** respectivamente.

2. Ejecute el comando ***certutil -addstore –f Root carootfiuba.crl*** en una consola de sistema con privilegios de administrador. Asegúrese que el archivo se encuentre en la carpeta donde se ejecuta el comando, ejem. C:\users\administrator\desktop

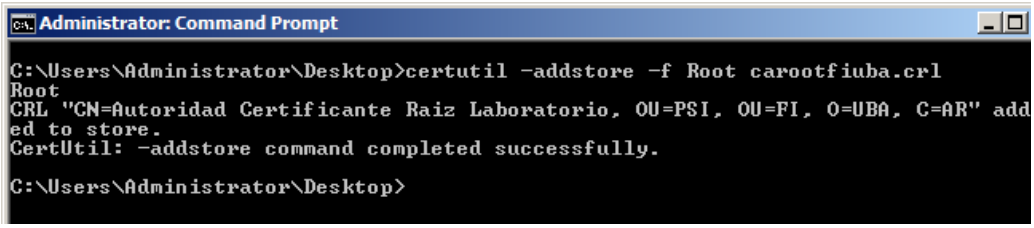


Figura 25. Almacenamiento de la CRL en la CA Integrada

3. Ejecute el comando ***certutil -addstore –f Root carootfiuba.crt*** en una consola de sistema con privilegios de administrador. Asegúrese que el archivo se encuentre en la carpeta donde se ejecuta el comando, ejem. C:\users\administrator\desktop

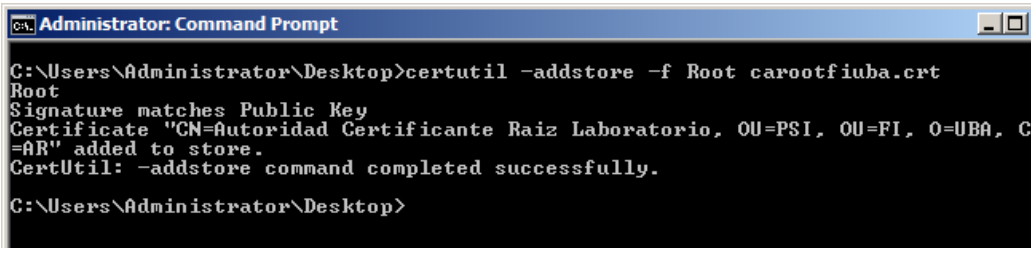


Figura 26. Almacenamiento del Certificado Raíz en la CA Integrada

4. Inicie la consola de administración de la CA seleccionando ***Inicio → Administration tools → Certification Authority***

5. **Importante:** El servicio está detenido. Seleccione ***Install CA Certificate…*** que se encuentra en el menú ***All Tasks*** al presionar con el botón derecho del mouse en ***Autoridad Certificante Integrada.***

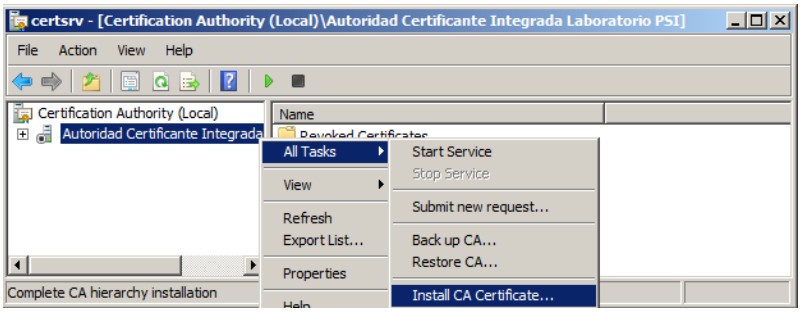


Figura 27. Consola de administración de la CA Integrada

6. Al ser requerido, proporcione el archivo que contiene el certificado firmado por la CA raíz (archivo .p7b obtenido de la Autoridad Certificante Raiz).

7. Inicie el servicio de la CA Integrada.

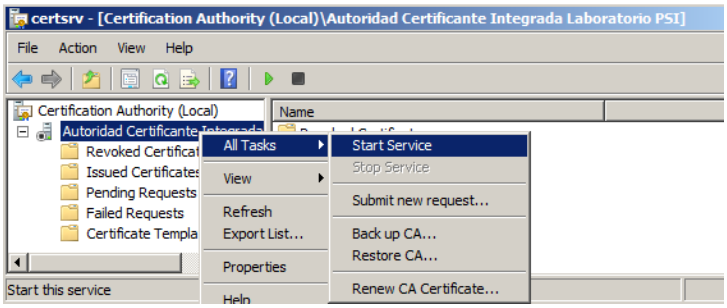


Figura 28. Inicio del servicio de la CA Integrada

Verificaciones del proceso de instalación de la CA operacional.

Verifique que se ha creado el certificado de la CA operacional.

1. Inicie la consola de administración de la CA seleccionando ***Inicio → Administration tools → Certification Authority***

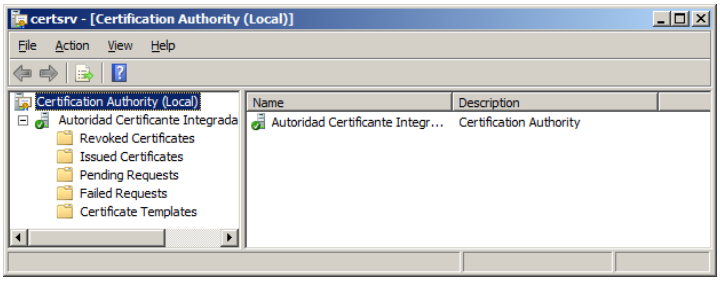


Figura 29. Consola de administración de la CA Integrada.

2. Con el botón derecho del mouse seleccione ***Autoridad Certificante Integrada*** y seguidamente la opción ***Properties*** y a continuación el botón ***View Certificate.***

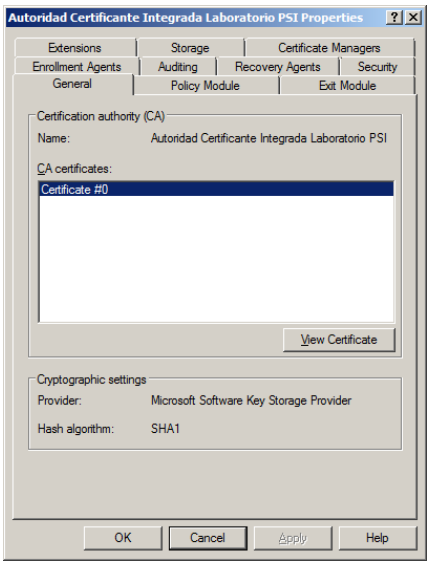


Figura 30. Propiedades de la CA

3. Verifique que el nombre del que emitió (***Issued to***) corresponde a: ***Autoridad Certificante Raiz Laboratorio*** y para quien fue emitido

(***Issued by***) corresponde a: ***Autoridad Certificante Integrada*** esto indica que el certificado fue firmado por la CA Raíz.

4. Verifique la vigencia del certificado.

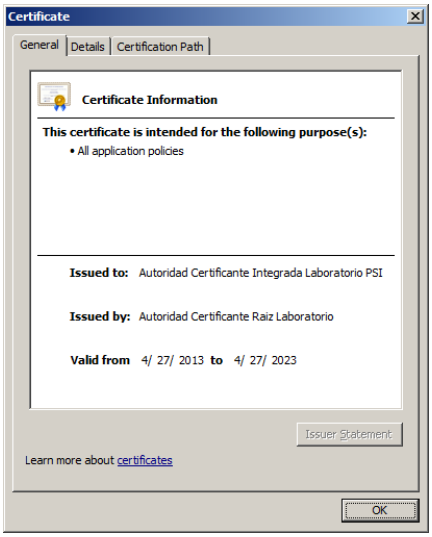


Figura 31. Propiedades del certificado de la CA Integrada.

5. Verifique que la llave pública tiene un tamaño de 2048 bits. Y que las rutas ***HTTP*** para la ***CDP*** y ***AIA*** se encuentran en los atributos de los certificados.

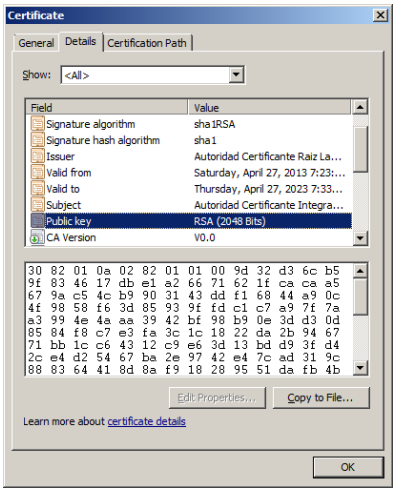


Figura 32. Atributo del tamaño de la llave pública.

6. Compruebe que en la viñeta ***Certification Path*** se encuentran todos los certificados de la jerarquía que forman la confianza.

Figura 33. Ruta de certificación

Laboratorio 2: Creación de una autoridad certificante (AC) Raíz y AC subordinada en Linux para la FCE.

Objetivo

Crear en Linux Debian una AC raíz y AC subordinada en Linux para la FCE, utilizando para ello OpenSSL. La AC raíz de la FCE firmara el certificado de la AC subordinada de la FCE. Además, la AC Subordinada proporcionará el servicio de emisión de certificados para los usuarios finales.

Una AC raíz, es el inicio de la cadena de confianza de una jerarquía de certificados digitales en una organización. Esta denominación se adquiere al emitir un certificado digital que se firma así mismo (autofirmado). Normalmente es un servidor que debe ser apagado y almacenado en una bóveda de seguridad una vez finalizado el proceso de firma de la AC subordinada o intermedia (autoridad que se encuentra en el siguiente nivel de la jerarquía) y generación de la CRL.

La AC subordinada, normalmente es un servidor que debe ser apagado y almacenado en una bóveda de seguridad una vez finalizado el proceso de firma de la AC operacional (autoridad que se encuentra en el siguiente nivel de la jerarquía) y generación de la CRL.

Nota: A pesar que este es un servidor que se mantiene apagado, considere que se requiere que los archivos que contienen la lista de revocación (CRL) y de acceso a la información de autoridad (AIA) son requeridos, por lo que debe disponer de un servidor web para almacenar y publicar estos archivos. En estos laboratorios se utiliza la URL **http://webrsrv.fce.uba.ar/publico**.

La AC operativa debe generar una lista de revocación de certificados (CRL) en lapsos de tiempo coherentes a las necesidades del negocio. A diferencia de la AC raíz que los tiempos de generación CRL son relativamente más largos. Los certificados de los usuarios finales están expuestos a una mayor cantidad de amenazas por lo que los tiempos de generación de la CRL deben ser cortos. Así mismo esta CRL debe poder ser accedida desde todos los equipos que tienen las aplicaciones y servicios de la organización,

por lo que se debe disponer de un servidor web para almacenar y publicar este archivo. En estos laboratorios se utiliza la AC subordinada como una AC operativa.

Proceso de creación de la autoridad certificante raíz

Para este proceso se utilizara el Linux Live CD para los laboratorios de seguridad de la información, por lo que se debe crear una máquina virtual para iniciar este entorno.

Nota: Asegúrese que la fecha y hora del sistema operativo es correcto. Si no lo es utilice el comando date set. Ejem:

date --set aaaa-mm-dd

date --set hh:mm:ss

1. Cree un directorio denominado ***pki*** y dentro de este el directorio ***etc***
2. Dentro del directorio ***pki/etc*** almacenar los archivos

    a. root-ca.conf (contiene el script de la AC raíz)
    b. subca-fce.conf (contiene el script de la AC subordinada)
    c. server.conf (contiene el script para la generación de un certificado de servidor).

3. Agregue la identificación de su grupo en el parámetro commonName del archivo **pki/etc/root-ca.conf**

    Ejemplo: commonName = "FCE Root CA Grupo 1"

4. Agregue la identificación de su grupo en el parámetro commonName del archivo **pki/etc/ subca-fce.conf**

    Ejemplo: commonName = "FCE SubCA Grupo 1"

Los siguientes comandos deben ejecutarse desde la ubicación ***/pki***

5. Ejecute los siguientes comandos para crear la estructura de directorios de la AC Raíz.

    Crypto:~/pki#**mkdir -p ca/root-ca-fce/private ca/root-ca-fce/db crl certs**

    Crypto:~/pki#**chmod 700 ca/root-ca-fce/private**

6. Ejecute los siguientes comandos para crear la estructura de archivos para la base de datos.

   Crypto:~/pki#**cp /dev/null ca/root-ca-fce/db/root-ca-fce.db**

   Crypto:~/pki#**cp /dev/null ca/root-ca-fce/db/root-ca-fce.db.attr**

   Crypto:~/pki#**echo 01 > ca/root-ca-fce/db/root-ca-fce.crt.srl**

   Crypto:~/pki#**echo 01 > ca/root-ca-fce/db/root-ca-fce.crl.srl**

7. Ejecute el siguiente comando para crear la solicitud de la AC Raíz.

   Crypto:~/pki#**openssl req -new -config etc/root-ca.conf -out ca/root-ca-fce.csr -keyout ca/root-ca-fce/private/root-ca-fce.key**

   Para proteger la llave privada se solicita una contraseña utilice la palabra: ***root***

8. Ejecute los siguientes comandos para firmar el certificado de la AC Raíz

   Crypto:~/pki#**openssl ca -selfsign -config etc/root-ca.conf -in ca/root-ca-fce.csr -out ca/root-ca-fce.crt -extensions root_ca_ext**

   Para proteger la llave privada se solicita una contraseña utilice la palabra: ***root***

   Seguidamente se le solicita que confirme firmar el certificado:

   Sign the certificate? [y/n]:y

   Y a continuación la confirmación de almacenar los cambios:

   1 out of 1 certificate requests certified, commit? [y/n]y

Proceso de creación de la autoridad certificante subordinada

1. Ejecute los siguientes comandos para crear la estructura de directorios de la AC Subordinada

   Crypto:~/pki#**mkdir -p ca/subca-fce/private ca/subca-fce/db crl certs**

   Crypto:~/pki#**chmod 700 ca/subca-fce/private**

2. Ejecute los siguientes comandos para crear la estructura de archivos para la base de datos

   Crypto:~/pki#**cp /dev/null ca/subca-fce/db/subca-fce.db**

   Crypto:~/pki#**cp /dev/null ca/subca-fce/db/subca-fce.db.attr**

Crypto:~/pki#**echo 01 > ca/subca-fce/db/subca-fce.crt.srl**

Crypto:~/pki#**echo 01 > ca/subca-fce/db/subca-fce.crl.srl**

3. Ejecute el siguiente comando para crear la solicitud de la AC Subordinada

   Crypto:~/pki#**openssl req -new -config etc/subca-fce.conf -out ca/subca-fce.csr -keyout ca/subca-fce/private/subca-fce.key**

   Para proteger la llave privada se solicita una contraseña utilice la palabra: ***subca***

4. Ejecute el siguiente comando para crear el certificado de la AC Subordinada

   Crypto:~/pki#**openssl ca -config etc/root-ca.conf -in ca/subca-fce.csr -out ca/subca-fce.crt -extensions signing_ca_ext**

   Este certificado debe ser firmado por la AC raíz por lo que al solicitársele, ingrese la clave de la AC raiz: ***root***

   Seguidamente se le solicita que confirme firmar el certificado:

   Sign the certificate? [y/n]:y

   Y a continuación la confirmación de almacenar los cambios:

   1 out of 1 certificate requests certified, commit? [y/n]y

Proceso de creación de un certificado de servidor

1. Ejecute los siguientes comandos para crear una solicitud para un certificado de servidor

   Crypto:~/pki#**SAN=DNS:websrv.fce.uba.ar**

   Crypto:~/pki#**openssl req -new -config etc/server.conf -out certs/websrv.fce.ar.csr -keyout certs/websrv.fce.ar.key**

Complete de acuerdo a la siguiente información:

1. Domain Component (eg, com) []:AR
2. Domain Component (eg, company) []:UBA
3. Domain Component (eg, pki) []:FCE
4. Organization Name (eg, company) []:Universidad de Buenos Aires
5. Organizational Unit Name (eg, section) []:

6. Common Name (eg, FQDN) []:websrv.fce.uba.ar

2. Ejecute el siguiente comando para crear el certificado del servidor:

   Crypto:~/pki#**openssl ca -config etc/subca-fce.conf -in certs/websrv.fce.ar.csr -out certs/websrv.fce.ar.crt -extensions server_ext**

   Este certificado debe ser firmado por la AC subordinada por lo que al solicitársele, ingrese la clave de la AC subordinada: ***subca***

   Seguidamente se le solicita que confirme firmar el certificado:

   Sign the certificate? [y/n]:y

   Y a continuación la confirmación de almacenar los cambios:

   1 out of 1 certificate requests certified, commit? [y/n]y

3. Ejecute los siguientes comandos para generar el archivo PEM para el Apache web server

   Crypto:~/pki#**cat certs/websrv.fce.ar.key certs/websrv.fce.ar.crt >certs/websrv.fce.ar.pem**

Proceso de configuración del Apache para una conexión SSL

1. Para habilitar el soporte de SSL ejecute el siguiente comando:

   Crypto:~/pki#**a2enmod ssl**

2. Crear el directorio ssl dentro de /etc/apache2/

   Crypto:~/pki# **mkdir /etc/apache2/ssl**

3. Copiar el certificado de servidor en la ruta: /etc/apache2/ssl

   Crypto:~/pki# **cp certs/websrv.fce.ar.pem /etc/apache2/ssl**

   Nota: El certificado se genera bajo el nombre: websrv.fce.ar.pem en el directorio: /pki/certs

4. Editar el archivo /etc/apache2/ports.conf para que el servidor habilite el puerto TCP 443 (Cambiar: Listen 80 por: Listen 443)

   Crypto:~/pki#**vi /etc/apache2/ports.conf**

5. Editar el archivo 000-default que se encuentra en /etc/apache2/sites-enabled/

   Crypto:~/pki#**vi /etc/apache2/sites-enabled/000-default**

   Cambiar: NameVirtualHost * por NameVirtualHost *:80

   Cambiar: <VirtualHost *> por <VirtualHost *:80>

   Al final agregar una nueva entrada:

   <VirtualHost *:443>

   ServerName websrv.fce.uba.ar

   DocumentRoot /var/www/

   ErrorLog /var/log/apache2/error.log

   CustomLog /var/log/apache2/access.log combined

   SSLEngine on

   SSLCertificateFile /etc/apache2/ssl/websrv.fce.ar.pem

   </VirtualHost>

6. Reiniciar el servicio de Apache

   Crypto:~/pki#**/etc/init.d/apache2 force-reload**

7. Comprobar desde la **Autoridad Certificante Subordinada** que se tiene acceso al servidor web por medio de la url https://websrv.fce.uba.ar

   Nota: para realizar esta comprobación se requiere editar el archivo ***hosts*** que se encuentra en c:\windows\system32\drivers\etc de la **Autoridad Certificante Integrada.** Utilice la consola de comandos con privilegios de administrador.

   Agregar lo siguiente:

   <Dirección IP del Linux> websrv.fce.uba.ar

8. Debe salir la alerta que indica que el certificado presentado no fue emitido por una autoridad certificante valida.

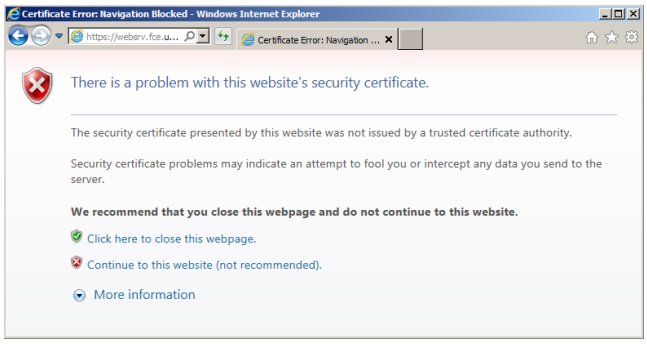


Figura 1. Alerta de seguridad

Nota: debido a que los almacenes: Autoridades Certificantes Raíz de Confianza y Autoridades Intermedias de confianza (repositorios propios del sistema operativo) no tienen los certificados de la jerarquía FCE el error presentado es normal.

Laboratorio 3: Proceso de Certificación Cruzada entre la Autoridad Certificante (CA) Subordinada Integrada con ADS FI y CA subordinada Linux OpenSSL FCE.

Objetivo

Efectuar el procedimiento para obtener un certificado cruzado con el propósito de lograr la interoperabilidad de dos jerarquías PKI.

En las siguientes secciones se explica el procedimiento para la creación, configuración y ejecución de tareas que conllevan la creación de un certificado cruzado entre Autoridades Certificantes.

Los componentes esenciales de este proceso son:

- Creación de la plantilla **Cross Certification Enrollment Agent**.
- Incorporación de plantillas **Cross Certification Enrollment Agent** y **Cross Certificate Authority** a la lista de emisión de certificados.
- Emisión del certificado para el Agente **Cross Certification Enrollment Agent**.
- Creación y parametrización del archivo de políticas de certificación (policy.inf)
- Proceso de firmado de la solicitud del certificado (req)
- Emisión del certificado cruzado (firmado de la solicitud con la llave privada de la Autoridad Certificante).

Creación de la plantilla del Agente para la solicitud de firmado (req)

Una vez establecida la Autoridad Certificante subordinada integrada con ADS (laboratorio 1), acceda a la consola de administración, Startup → Administrative tools → Certification Authority. Seleccione **Certificate Templates** utilizando el botón derecho del mouse y posteriormente la opción **Manage.**

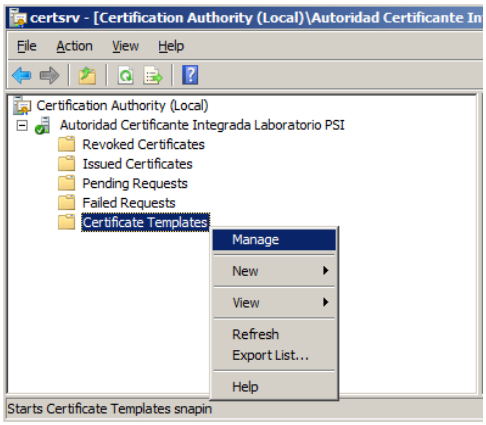


Figura 1. Consola de Administracion de la CA

Se abre la **Consola de Plantillas de Certificados**, donde se procedera a duplicar la plantilla de **Enrollment Agent,** seleccionando con el botón derecho del mouse esta plantilla y a continuacion la opción **Duplicate Template**.

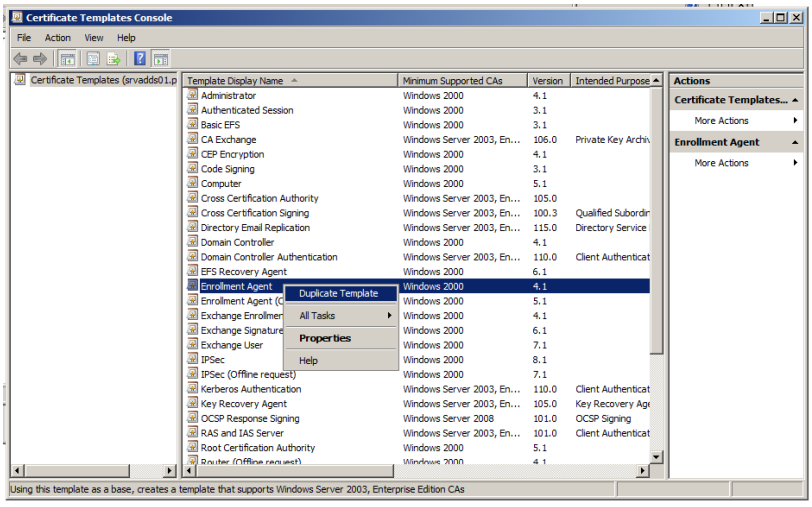


Figura 2. Consola de plantillas de certificados

Se presenta la ventana de advertencia indicando que la plantilla puede ser creada utilizando opciones avanzadas. No todas las Autoridades Certificantes son compatibles con estas propiedades, por lo que para los

fines de este laboratorio seleccione Windows 2003 Server, Enterprise Edition.

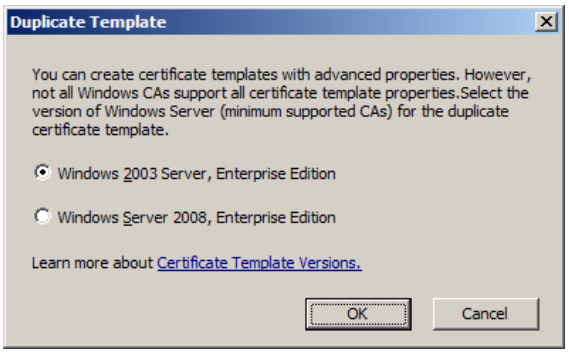


Figura 3. Opciones avanzadas

Se presentan las propiedades relativas a la nueva plantilla. En la opción **Template display name**, coloque un nombre descriptivo en función de las necesidades. (eje. Cross Certification Signing).

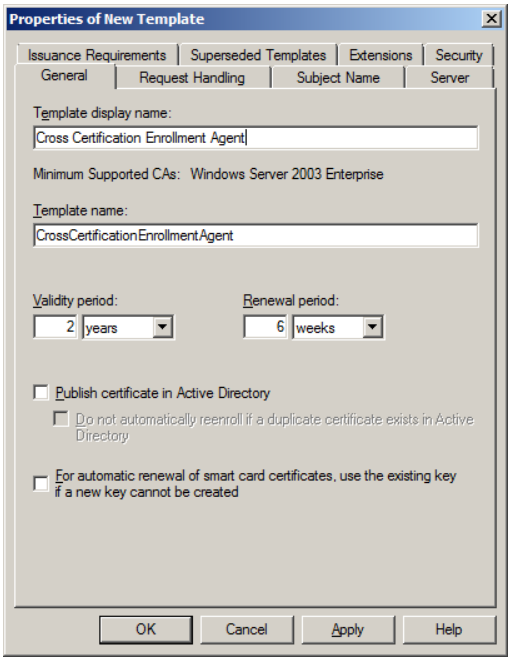


Figura 4. Propiedades de la nueva plantilla

El establecimiento de los parametros dependeran de las necesidades de cada situación. En los siguientes pasos se muestran los parametros mínimos que deben establecerse.

Seleccione la viñeta **Extensions** y seguidamente, edite la opción **Applicacion Policies** utilizando el botón **Edit.**

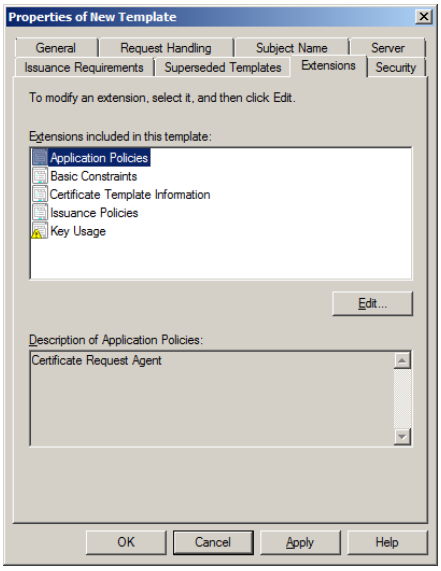


Figura 5. Extensiones de la nueva plantilla

En la ventana **Edit Application Policies Extension**, seleccione la política de aplicación **Certificate Request Agent** y seleccione el botón **Remove.**

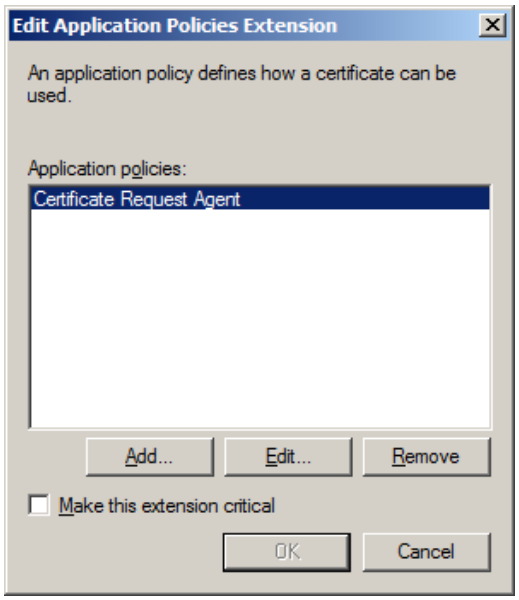


Figura 6. Extension de políticas de aplicación

Seguidamente seleccione el boton **Add**, agregue la política de aplicación **Qualified Subordination** y seguidamente el botón **OK.**

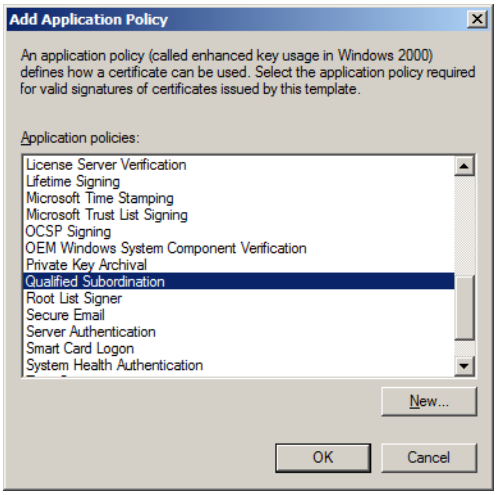


Figura 7. Adición de políticas de aplicación

En la lista políticas de aplicación, únicamente deberá observarse **Qualified Subordination.**

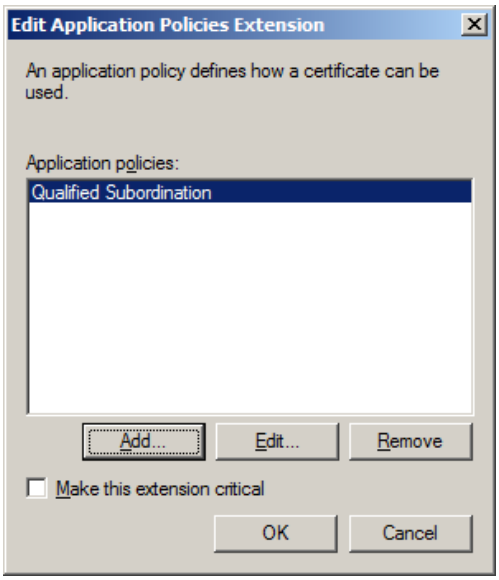


Figura 8. Edición de políticas de aplicación

Seleccione el botón **OK** y seguidamente el botón **OK** de la ventana **Propierties of New Template.**

Incorporación de las plantillas de certificación cruzada a la lista de emisión de certificados

En la Consola de la Autoridad Certificante, seleccione **Certificate Templates** utilizando el botón derecho del mouse, seguidamente la opción **New** y posteriormente **Certificate Template to Issue.**

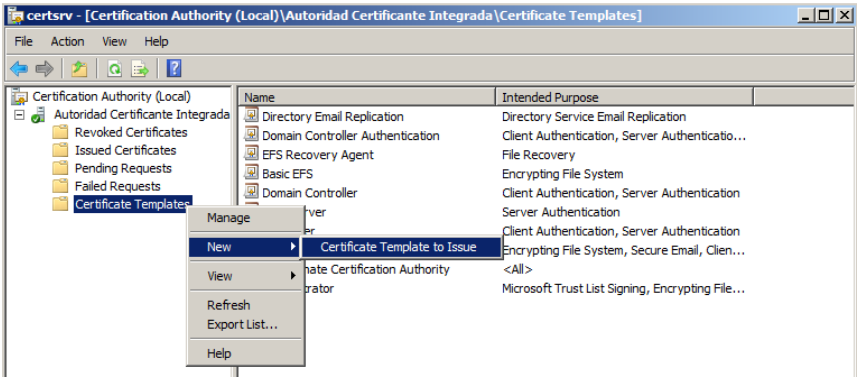


Figura 9. Consola de Administracion de la CA

De la lista **Enable Certificates Templates**, localice las plantillas **Cross Certification Authority** y **Cross Certification Enrollment Agent** (Utilice la tecla Ctrl para seleccionar más de una plantilla). Posteriormente presione sobre el botón **OK**.

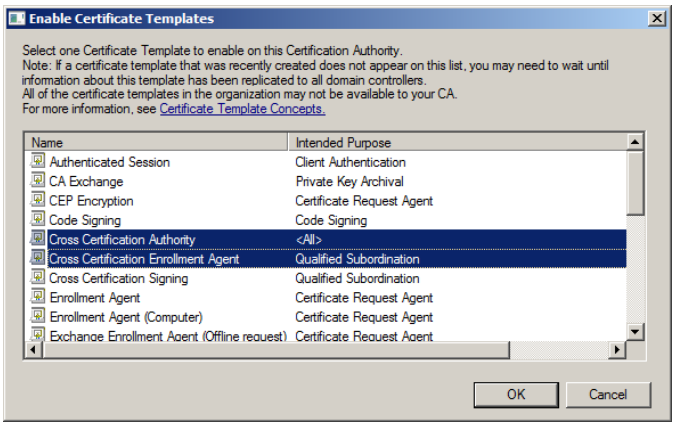


Figura 10. Habilitación de plantillas de certificados

Asegúrese que las nuevas plantillas aparecen en la lista de **Plantillas de Certificados.**

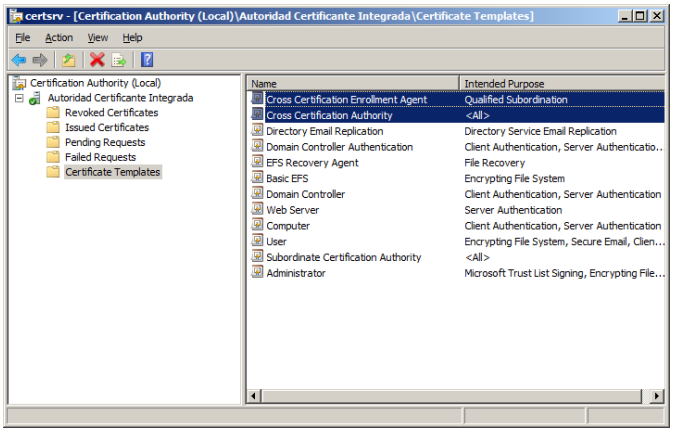


Figura 11. Consola de Administracion de la CA

Emisión del certificado Cross Certification Enrollment Agent

En la consola de administración de certificados (certmgr.msc), seleccione la opción **Request New Certificate**, como corresponde en la siguiente imagen.

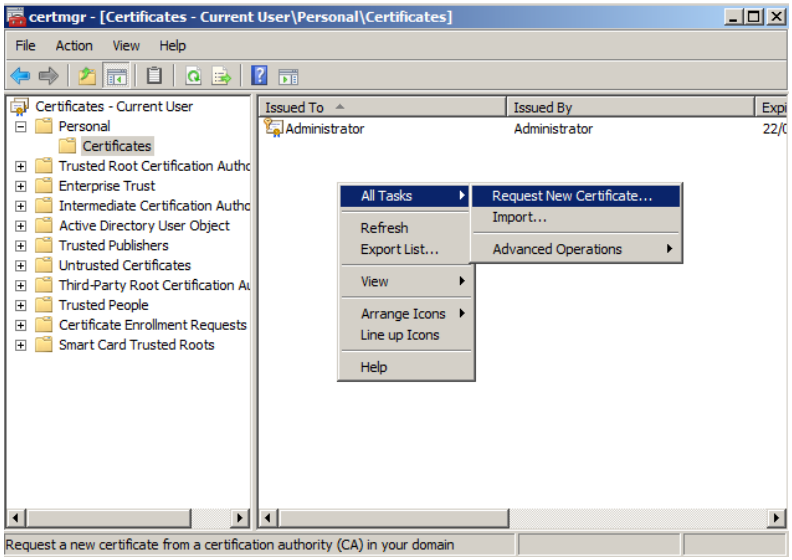


Figura 12. Almacén de certificados personales

Se iniciara el asistente de Enrolamiento de Certificados, seleccione el botón **Next** hasta llegar a la ventana **Request Certificates.**

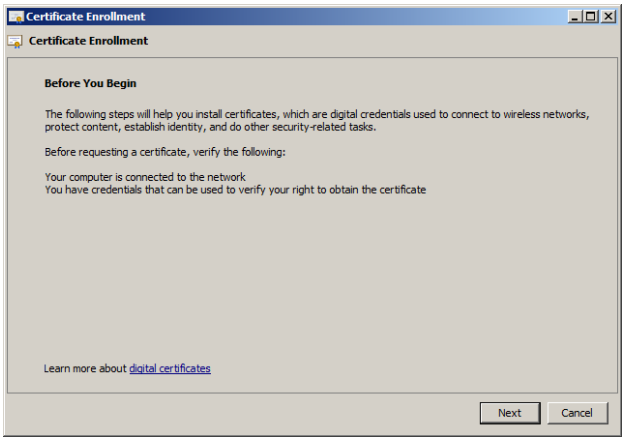


Figura 13. Asistente de solicitud de certificados

Seleccione la casilla **Cross Certification Enrollment Agent** (esta plantilla debió haberse agregado en la sección anterior).

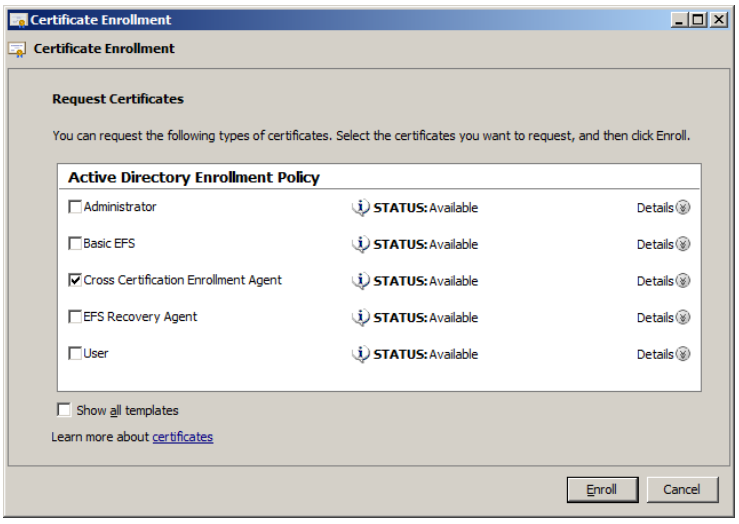


Figura 14. Selección de emisión de certificados

Asegúrese que la creación del agente se efectuó satisfactoriamente, verificando el **STATUS: Succeeded** conforme a la siguiente imagen.

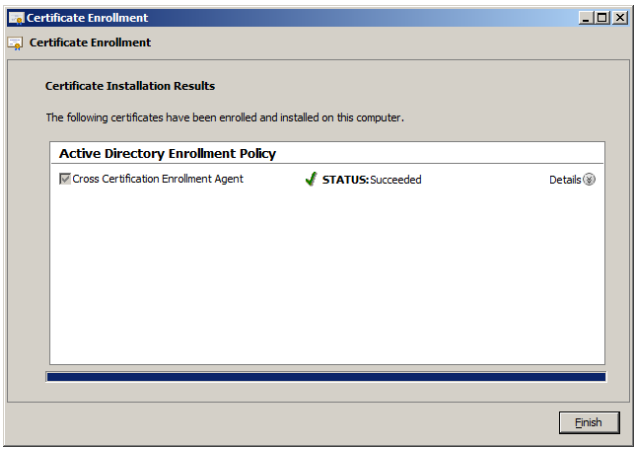


Figura 15. Estado de emisión de certificado

Verifique que el agente se ha agregado a la lista de certificados emitidos y que el propósito corresponda a **Qualified Subordination**. En este caso el usuario **Administrador** es el que tiene el permiso de utilizar este agente.

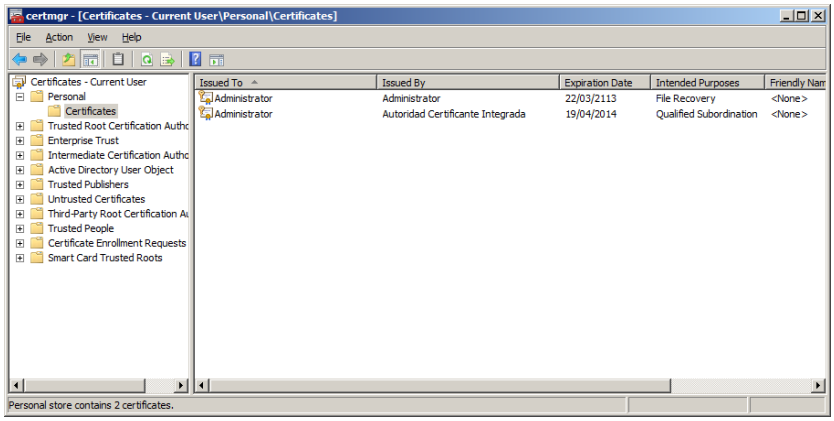


Figura 16. Verificación de la emisión del certificado

Preparación y creación del archivo de políticas (policy.inf)

El archivo de políticas (policy.inf) está compuesto por secciones que establecen algunos parámetros que determinan el comportamiento del certificado cruzado entre las Autoridades Certificantes.

Este es un archivo de texto cuya ubicación y extensión no es específica, por lo que puede ser ubicado en cualquier directorio del servidor y puede tener cualquier extensión, se recomienda que esta última sea **.inf**

con el propósito de mantener un estándar en las extensiones de archivos utilizados para la creación de Autoridades Certificantes.

Algunos parámetros se utilizan como reglas para establecer las restricciones que el certificado cruzado valida en los certificados presentados por los servidores. A continuación se muestra el archivo utilizado en la Certificación Cruzada de este laboratorio.

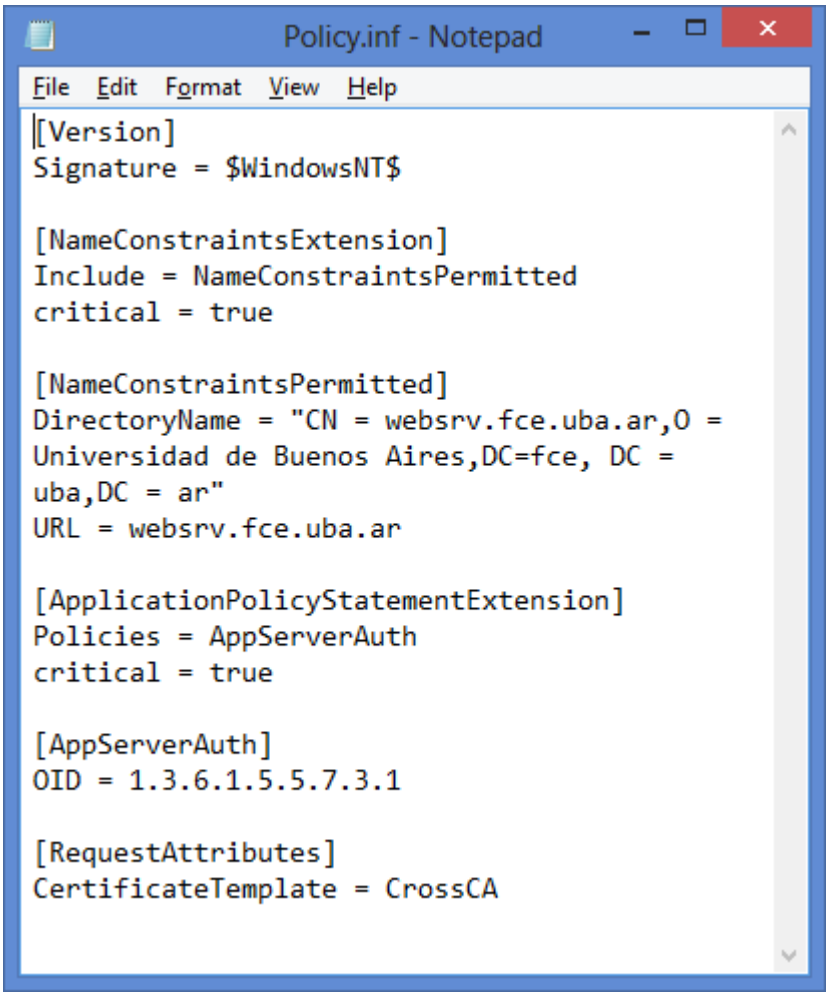


Figura 17. Archivo policy.inf

A continuación se describen las secciones utilizadas en el archivo policy.inf.

Sección/Campo	**Parámetro**	**Descripción**
[Version]	"$Windows NT$"	Indica el

Signature=		sistema operativo para el cual este archivo es válido. Para la familia de servidores Windows se indica el parámetro.
[NameConstraintsExtension]	Include	Indica las restricciones que se incluyen, si la expresión concuerda, otorga el permiso de uso.
	Exclude	Indica las restricciones que se excluyen, si la expresión concuerda, deniega el permiso de uso.
	Critical [yes/no]	Indica si el parámetro es crítico, si es “yes” aparece el símbolo de un triángulo amarillo.

[BasicConstraintsExtension]	PathLength	Indica el número de niveles de la jerarquía que la certificación cruzada (bajo este nivel) reconocerá como válida.
[ApplicationPolicyStatementExtention]	Policies	Indica los tipos de certificados que serán reconocidos por la Certificación Cruzada.
	Critical [yes/no]	Indica si el parámetro es crítico, si es “yes” aparece el símbolo de un triángulo amarillo.
[RequestAttributes]	CertificateTemplate	Indica el nombre de la plantilla que se usará para firmar la solicitud de Certificación Cruzada

Proceso de emisión del certificado cruzado

Mediante la ejecución de la línea de comando **certreq –policy** se procesa la solicitud de certificación cruzada, de acuerdo al siguiente procedimiento:

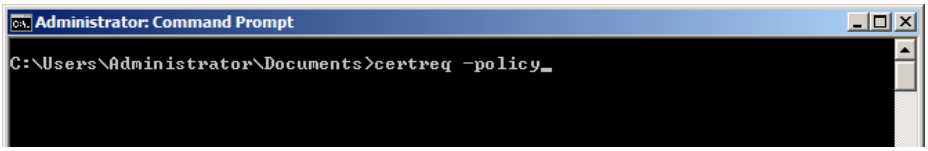


Figura 18. Generación de solicitud

Al ejecutar el comando, se solicitara la ubicación del archivo **subca-fce.crt** que contiene el certificado de la **Autoridad Certificante** subordinada de la FCE, este archivo se encuentra en el directorio ***/pki/ca/*** (laboratorio 2).

Al seleccionar el botón **Open**, se solicita la ubicación del archivo **policy.inf** (archivo que contiene las reglas correspondientes). Seguidamente seleccione el botón **Open.**

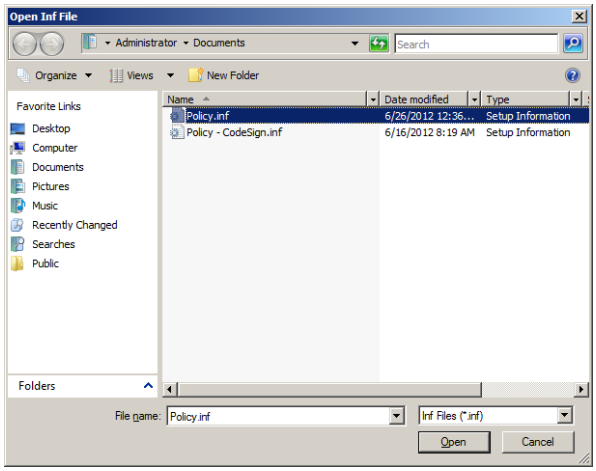


Figura 19. Ubicación del archivo policy.inf

Este proceso busca la llave privada correspondiente al **Agente de Certificación Cruzada.**

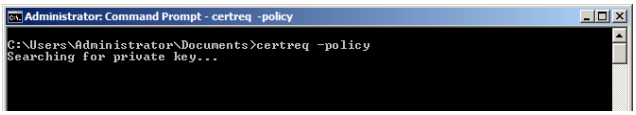


Figura 20. Firmado de la solicitud

Seleccione el agente correspondiente. Puede seleccionar la opción **Click here to view certificate properties** para ver más detalles del certificado. Asegúrese que el certificado seleccionado tenga el propósito **Qualified Subordination, seguidamente seleccione** el botón **OK.**

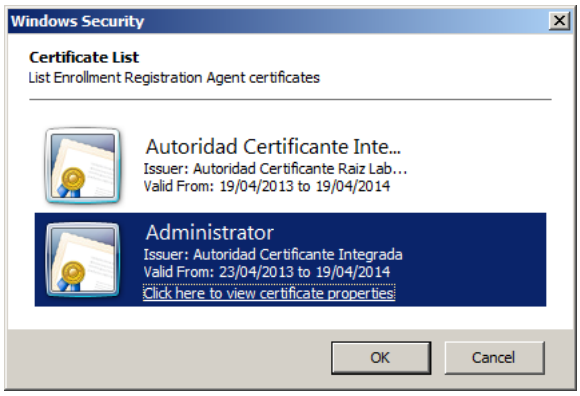


Figura 21. Selección del certificado de firma

Seguidamente se solicita un nombre para el archivo de solicitud que se ha firmado con la llave privada del Agente de Certificación Cruzada, utilice el nombre ***fce-subca-request***. Al seleccionar el botón **Save**, el archivo está listo para ser enviado a la Autoridad Certificante Integrada de la **FI** para que este sea firmado con la llave privada de ésta.

Emisión del Certificado Cruzado

Ingrese a la consola de la Autoridad Certificante Integrada (puede utilizar el comando certsrv.msc), seleccione con el botón derecho el mouse sobre el identificador que corresponde a la Autoridad Certificadora

(Autoridad Certificante Integrada Laboratorio PSI), seleccione **All Tasks** y seguidamente **Submit new request…**

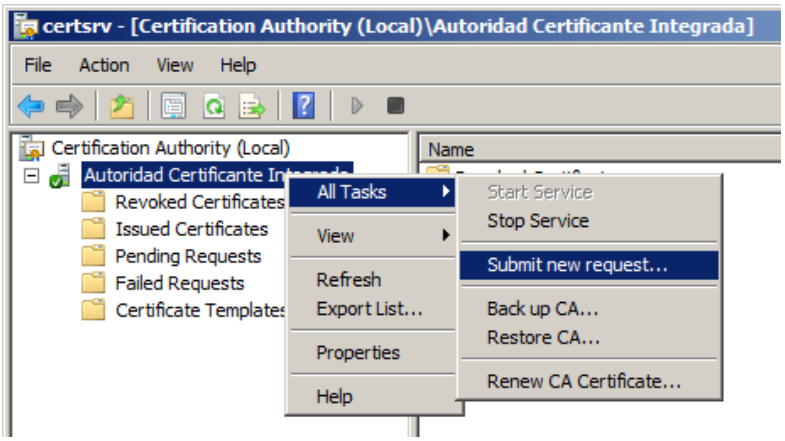


Figura 22. Envío de solicitud de certificado

Proporcione el archivo que corresponde a la solicitud firmada por el **Agente de Certificación Cruzada** (archivo **fce-subca-request.req**) y presione el botón **Open.**

El proceso firma con la llave privada de la AC Subordinada la solicitud y se obtiene el **Certificado Cruzado**, seguidamente solicita la ubicación para almacenarlo**.** Utilice el nombre ***fce-subca-cross-sign*.**

Verificación de las propiedades del certificado cruzado

El archivo se almacena con extensión **.cer**. Al ejecutar este archivo, se muestran las propiedades del **Certificado Cruzado**, en la viñeta **General** se muestran las propiedades del certificado junto con los propósitos para los cuales el certificado ha sido destinado, a quien se ha emitido (FCE SubCA), quien lo emitió (Autoridad Certificante Integrada Laboratorio PSI de la FI) y la fecha de validez.

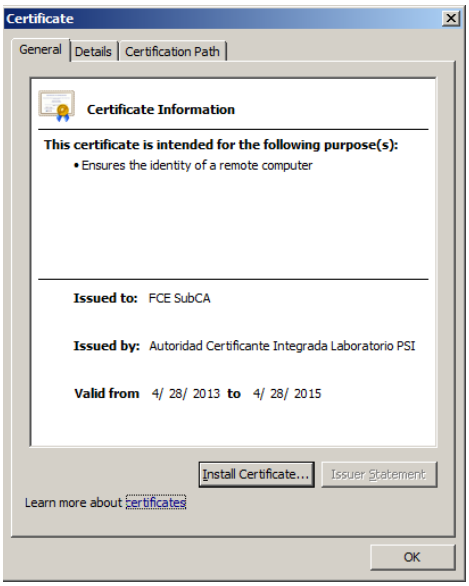


Figura 23. Verificación de la viñeta general

En la viñeta **Details**, se muestran el valor del **Subject Key Identifier** que debe corresponder al certificado de la **Autoridad Certificante Subordinada de FCE** y el **Authority Key Identifier** debe corresponder a la **Autoridad Certificante Integrada FI**.

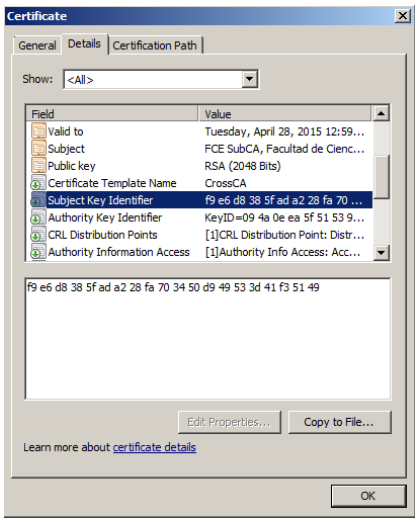


Figura 24. Verificación de la viñeta de detalles

La viñeta **Certification Path** presenta la cadena de certificación, donde se muestra la jerarquía correspondiente a la FI.

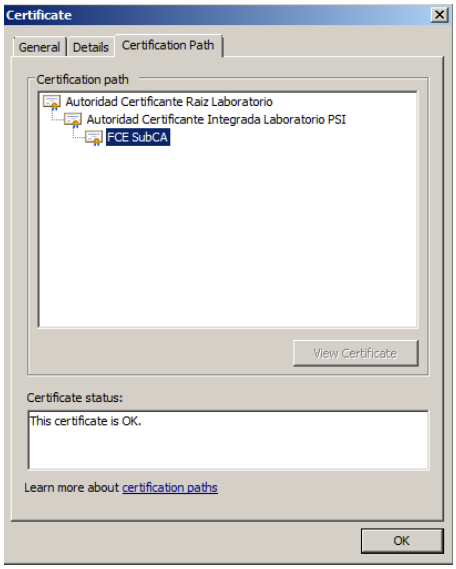


Figura 25. Verificacion de la viñeta de Rutas de certificados

Distribución de la cadena de certificación.

El funcionamiento de la Certificación Cruzada radica en una distribución o despliegue adecuado de la cadena de certificación. Esta cadena puede ser distribuida por medio del **Group Policy** en el caso de estaciones con Windows.

El siguiente procedimiento se debe efectuar en todos los equipos que van a interactuar con el servidor web de FCE (Servidor Linux Debian con Apache, configurado en el laboratorio 2) Instale el certificado cruzado en el almacén de ***Autoridades Certificantes Intermedias*** de la ***Autoridad Certificante Integrada Laboratorio PSI***

Seleccione el botón ***Install*** que se encuentra en la viñeta ***General*** de las propiedades del certificado.

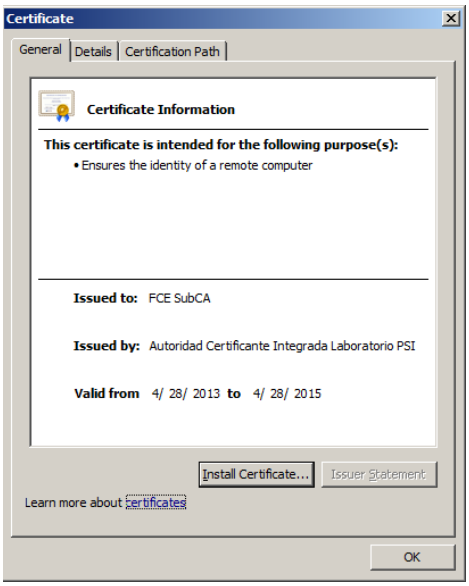


Figura 26. Instalación del certificado cruzado

Se inicia el asistente para importar certificados, seleccione el botón ***Next*** y en la siguiente ventana seleccione la opción ***Place all certificates in the following store*** seguidamente el botón ***Browse.***

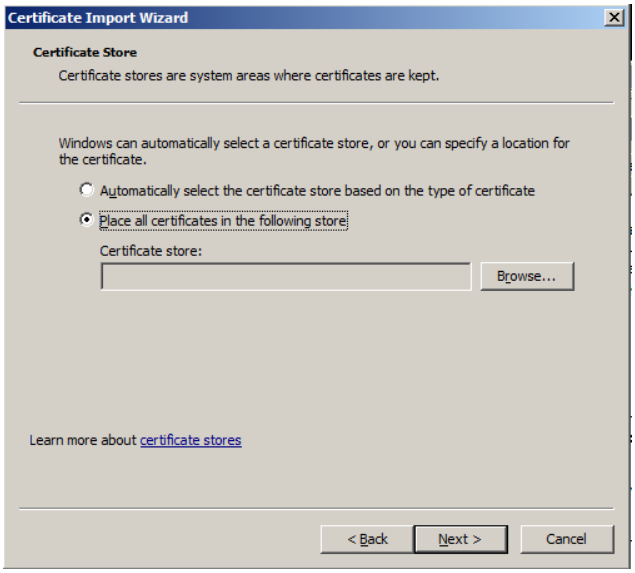


Figura 27. Selección del almacén

Seleccione el almacén denominado ***Intermediate Certification Authorities*** y a continuación el botón ***OK.***

Figura 28. Almacenes de certificados

Finalice con el asistente seleccionando el botón ***Next*** y ***Finish*** asegúrese de que aparezca la ventana de confirmación que indica que el certificado fue importado satisfactoriamente.

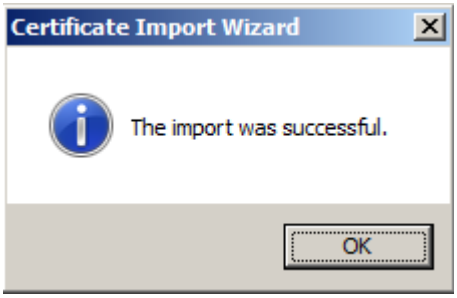


Figura 29. Instalación satisfactoria del certificado.

Compruebe que tiene acceso a la url **https://websrv.fce.uba.ar** y que no se presenta ninguna alerta de error de certificados.

Scripts utilizados para la generación de certificados con OpenSSL

Para facilitar el proceso de creación de la PKI de la FCE, se proporcionan los siguientes scripts que contienen los elementos necesarios para la creación de la CA Raíz y CA Subordinada, además se incluyen los scripts para la generación de certificados SSL y para uso de correo electrónico.

Estos scripts fueron tomados de la OpenSSL PKI Tutorial v1.0 ubicada en la URL http://pki-tutorial.readthedocs.org/en/latest/index.html consultada el 26 de abril de 2013.

CA Raíz de FCE

```
# Simple Root CA

# The [default] section contains global constants that can be referred to from
# the entire configuration file. It may also hold settings pertaining to more
# than one openssl command.

[ default ]
ca                = root-ca-fce         # CA name
dir               = .                   # Top dir

# The next part of the configuration file is used by the openssl req command.
# It defines the CA's key pair, its DN, and the desired extensions for the CA
# certificate.

[ req ]
default_bits          = 2048              # RSA key size
encrypt_key           = yes               # Protect private key
default_md            = sha1              # MD to use
```

```
utf8                = yes               # Input is UTF-8
string_mask         = utf8only          # Emit UTF-8 strings
prompt              = no                # Don't prompt for DN
distinguished_name  = ca_dn             # DN section
req_extensions      = ca_reqext         # Desired extensions

[ ca_dn ]
0.domainComponent       = "AR"
1.domainComponent       = "UBA"
2.domainComponent       = "FCE"
organizationName        = "Universidad de Buenos Aires"
organizationalUnitName  = "Facultad de Ciencias Economicas"
commonName              = "FCE Root CA"

[ ca_reqext ]
keyUsage            = critical,keyCertSign,cRLSign
basicConstraints    = critical,CA:true
subjectKeyIdentifier    = hash

# The remainder of the configuration file is used by the openssl ca command.
# The CA section defines the locations of CA assets, as well as the policies
# applying to the CA.

[ ca ]
default_ca          = root_ca           # The default CA section

[ root_ca ]
certificate         = $dir/ca/$ca.crt       # The CA cert
private_key         = $dir/ca/$ca/private/$ca.key # CA private key
new_certs_dir       = $dir/ca/$ca           # Certificate archive
serial              = $dir/ca/$ca/db/$ca.crt.srl # Serial number file
crlnumber           = $dir/ca/$ca/db/$ca.crl.srl # CRL number file
```

```
database            = $dir/ca/$ca/db/$ca.db # Index file
unique_subject      = no                   # Require unique subject
default_days        = 3652                 # How long to certify for
default_md          = sha1                 # MD to use
policy              = match_pol            # Default naming policy
email_in_dn         = no                   # Add email to cert DN
preserve            = no                   # Keep passed DN ordering
name_opt            = ca_default           # Subject DN display options
cert_opt            = ca_default           # Certificate display options
copy_extensions     = none                 # Copy extensions from CSR
x509_extensions     = signing_ca_ext       # Default cert extensions
default_crl_days    = 365                  # How long before next CRL
crl_extensions      = crl_ext              # CRL extensions

# Naming policies control which parts of a DN end up in the certificate and
# under what circumstances certification should be denied.

[ match_pol ]
domainComponent     = match                # Must match 'simple.org'
organizationName    = match                # Must match 'Simple Inc'
organizationalUnitName  = optional         # Included if present
commonName          = supplied             # Must be present

[ any_pol ]
domainComponent     = optional
countryName         = optional
stateOrProvinceName     = optional
localityName        = optional
organizationName    = optional
organizationalUnitName  = optional
commonName          = optional
emailAddress        = optional
```

```
# Certificate extensions define what types of certificates the CA is able to
# create.

[ root_ca_ext ]
keyUsage              = critical,keyCertSign,cRLSign
basicConstraints      = critical,CA:true
subjectKeyIdentifier  = hash
authorityKeyIdentifier  = keyid:always

[ signing_ca_ext ]
keyUsage              = critical,keyCertSign,cRLSign
basicConstraints      = critical,CA:true,pathlen:0
subjectKeyIdentifier  = hash
authorityKeyIdentifier  = keyid:always

# CRL extensions exist solely to point to the CA certificate that has issued
# the CRL.

[ crl_ext ]
authorityKeyIdentifier  = keyid:always
```

CA Subordinada de FCE

```
# Simple Signing CA
# The [default] section contains global constants that can be referred to from
# the entire configuration file. It may also hold settings pertaining to more
# than one openssl command.

[ default ]
ca                  = subca-fce         # CA name
dir                 = .                 # Top dir
```

```
# The next part of the configuration file is used by the openssl req command.
# It defines the CA's key pair, its DN, and the desired extensions for the CA
# certificate.

[ req ]
default_bits           = 2048               # RSA key size
encrypt_key            = yes                # Protect private key
default_md             = sha1               # MD to use
utf8                   = yes                # Input is UTF-8
string_mask            = utf8only           # Emit UTF-8 strings
prompt                 = no                 # Don't prompt for DN
distinguished_name     = ca_dn              # DN section
req_extensions         = ca_reqext          # Desired extensions

[ ca_dn ]
0.domainComponent      = "AR"
1.domainComponent      = "UBA"
2.domainComponent      = "FCE"
organizationName       = "Universidad de Buenos Aires"
organizationalUnitName  = "Facultad de Ciencias Economicas"
commonName             = "FCE SubCA"

[ ca_reqext ]
keyUsage               = critical,keyCertSign,cRLSign
basicConstraints       = critical,CA:true,pathlen:0
subjectKeyIdentifier   = hash

# The remainder of the configuration file is used by the openssl ca command.
# The CA section defines the locations of CA assets, as well as the policies
# applying to the CA.
```

```
[ ca ]
default_ca            = signing_ca          # The default CA section

[ signing_ca ]
certificate           = $dir/ca/$ca.crt      # The CA cert
private_key           = $dir/ca/$ca/private/$ca.key # CA private key
new_certs_dir         = $dir/ca/$ca          # Certificate archive
serial                = $dir/ca/$ca/db/$ca.crt.srl # Serial number file
crlnumber             = $dir/ca/$ca/db/$ca.crl.srl # CRL number file
database              = $dir/ca/$ca/db/$ca.db # Index file
unique_subject        = no                   # Require unique subject
default_days          = 730                  # How long to certify for
default_md            = sha1                 # MD to use
policy                = match_pol            # Default naming policy
email_in_dn           = no                   # Add email to cert DN
preserve              = no                   # Keep passed DN ordering
name_opt              = ca_default           # Subject DN display options
cert_opt              = ca_default           # Certificate display options
copy_extensions       = copy                 # Copy extensions from CSR
x509_extensions       = email_ext            # Default cert extensions
default_crl_days      = 7                    # How long before next CRL
crl_extensions        = crl_ext              # CRL extensions

# Naming policies control which parts of a DN end up in the certificate and
# under what circumstances certification should be denied.

[ match_pol ]
domainComponent       = match                # Must match 'simple.org'
organizationName      = match                # Must match 'Simple Inc'
organizationalUnitName  = optional           # Included if present
commonName            = supplied             # Must be present
```

```
[ any_pol ]
domainComponent         = optional
countryName             = optional
stateOrProvinceName     = optional
localityName            = optional
organizationName        = optional
organizationalUnitName  = optional
commonName              = optional
emailAddress            = optional

# Certificate extensions define what types of certificates the CA is able to
# create.

[ email_ext ]
keyUsage                = critical,digitalSignature,keyEncipherment
basicConstraints        = CA:false
extendedKeyUsage        = emailProtection,clientAuth
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always

[ server_ext ]
keyUsage                = critical,digitalSignature,keyEncipherment
basicConstraints        = CA:false
extendedKeyUsage        = serverAuth,clientAuth
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always

# CRL extensions exist solely to point to the CA certificate that has issued
# the CRL.

[ crl_ext ]
authorityKeyIdentifier  = keyid:always
```

Generación de certificado SSL utilizado para servicio web FCE

```
# TLS server certificate request

# This file is used by the openssl req command. The subjectAltName cannot be
# prompted for and must be specified in the SAN environment variable.

[ default ]
SAN                 = DNS:websrv.fce.uba.ar    # Default value

[ req ]
default_bits          = 2048               # RSA key size
encrypt_key           = no                 # Protect private key
default_md            = sha1               # MD to use
utf8                = yes                # Input is UTF-8
string_mask           = utf8only           # Emit UTF-8 strings
prompt              = yes                # Prompt for DN
distinguished_name    = server_dn          # DN template
req_extensions        = server_reqext      # Desired extensions

[ server_dn ]
0.domainComponent     = "1. Domain Component       (eg, com)     "
1.domainComponent     = "2. Domain Component       (eg, company)  "
2.domainComponent     = "3. Domain Component       (eg, pki)     "
organizationName      = "4. Organization Name      (eg, company)  "
organizationalUnitName  = "5. Organizational Unit Name (eg, section)  "
commonName            = "6. Common Name            (eg, FQDN)    "
commonName_max        = 64

[ server_reqext ]
```

```
keyUsage              = critical,digitalSignature,keyEncipherment
extendedKeyUsage      = serverAuth,clientAuth
subjectKeyIdentifier  = hash
subjectAltName        = $ENV::SAN
```

Generación de certificado para correo electrónico FCE

```
# Email certificate request

# This file is used by the openssl req command. Since we cannot know the DN in
# advance the user is prompted for DN information.

[ req ]
default_bits          = 2048              # RSA key size
encrypt_key           = yes               # Protect private key
default_md            = sha1              # MD to use
utf8                  = yes               # Input is UTF-8
string_mask           = utf8only          # Emit UTF-8 strings
prompt                = yes               # Prompt for DN
distinguished_name    = email_dn          # DN template
req_extensions        = email_reqext      # Desired extensions

[ email_dn ]
0.domainComponent     = "1. Domain Component       (eg, com)     "
1.domainComponent     = "2. Domain Component       (eg, company) "
2.domainComponent     = "3. Domain Component       (eg, pki)     "
organizationName      = "4. Organization Name      (eg, company) "
organizationalUnitName= "5. Organizational Unit Name (eg, section) "
commonName            = "6. Common Name            (eg, full name)"
commonName_max        = 64
emailAddress          = "7. Email Address          (eg, name@fqdn)"
```

```
emailAddress_max        = 40

[ email_reqext ]
keyUsage                = critical,digitalSignature,keyEncipherment
extendedKeyUsage        = emailProtection,clientAuth
subjectKeyIdentifier    = hash
subjectAltName          = email:move
```

Articulo Laboratorio de confianza entre organizaciones utilizando Certificación Cruzada a TIBETS 2013

Laboratorio de confianza entre organizaciones utilizando certificacion cruzada

E.Milla, H.Pagola, A.Dams

***Abstract*— El presente trabajo describe una experiencia de laboratorio desarrollada para los estudiantes del Posgrado en Seguridad Informática de la UBA. Se han preparado ambientes operativos virtualizados que permitan experimentar e interactuar con sistemas operativos y servicios que proveen soluciones de interoperabilidad de forma segura entre organizaciones. Se le plantean al estudiante los modelos de confianza utilizando infraestructuras de clave pública (PKI). Los laboratorios orientan al estudiante en una serie de actividades que van desde la construcción del inicio de una cadena de confianza hasta el proceso de interactuar con aplicaciones que utilizan certificados.**

Para establecer una relación entre Autoridades Certificantes se le propone al estudiante el modelo de certificación cruzada que permite establecer reglas de acceso en forma arbitraria a uno o varios niveles de una jerarquía PKI, limitando de esta manera, el acceso a equipos, sitios web, direcciones de correo, etc., modificando el nivel de confianza que se establece de acuerdo a las necesidades de las organizaciones. Con lo anterior se evita que las organizaciones se vean forzadas a confiar en toda una jerarquía PKI cuando hacen el intercambio de certificados raíz y certificados intermedios entre ellas.

***Keywords*— Infraestructura de clave pública, certificación cruzada, certificados, pki, confianza.**

I. INTRODUCCIÓN

Hoy día las organizaciones utilizan certificados digitales para varios propósitos, que de forma relativa mejoran la seguridad y confiabilidad en sus entornos en comparación a los modelos tradicionales.

Edy Milla, Universidad de Buenos Aires (UBA), Buenos Aires, Argentina, edy.milla@gmail.com

Alberto Dams, Universidad de Buenos Aires (UBA), Buenos Aires, Argentina, albertodams@gmail.com

Hugo Pagola, Facultad de Ingeniería, Universidad de Buenos Aires (UBA), Buenos Aires, Argentina, hpagola@fi.uba.ar

Debido a las relaciones de negocio que con mayor frecuencia se establecen entre organizaciones, es necesario contar con una solución tecnológica que permita la interacción con la mayor confianza posible minimizando el esfuerzo.

Una de las soluciones que se utilizan para lograr este objetivo, es el modelo jerárquico de autoridades certificantes (AC). En este modelo se establece una AC raíz que debe ser común entre las organizaciones para posteriormente autorizar AC subordinadas, con la desventaja que al tener una AC raíz en común, se dificulta establecer límites en el nivel de confianza. Por lo que desde el punto de vista de seguridad, este modelo no es el más indicado para lograr este objetivo.

Las organizaciones que ya tienen una PKI implementada, pueden recurrir al modelo de certificación cruzada [11] en el que cada organización firma el o los certificados de una AC subordinada de la otra organización a un nivel arbitrario de la jerarquía para que exista confianza a partir de ese nivel, con la ventaja que el nivel de confianza se establece mediante construcción de reglas de acuerdo a las necesidades de la organización.

Para poner en práctica el modelo de certificación cruzada se han preparado los siguientes laboratorios:

- Construcción de una AC raíz en Windows Server 2008.
- Construcción de un servidor con Directorio Activo
- Construcción de una AC Subordinada Integrada con el Directorio Activo en Windows Server 2008.
- Construcción de una AC raíz y subordinada en Linux Debian utilizando Open SSL.
- Proceso de Certificación Cruzada, pruebas de funcionamiento y cuestionario.

.

II. OBJETIVOS

Se plantean una serie de objetivos cuyo propósito es llevar al estudiante a la ejercitación de lo aprendido en las clases teóricas, de manera que pueda interactuar con ambientes que en la actualidad existen en las organizaciones. Entre estos se encuentran:

- Familiarizar al estudiante con los conceptos de Infraestructura de llave Pública (PKI).
- Orientar en la Construcción de una Infraestructura de Clave Pública (PKI) [12] utilizando los sistemas operativos Linux Debian [13] con OpenSSL [14] y Windows Server 2008 [15].
- Mostrar la importancia que actualmente se le da a los certificados digitales en muchos entornos.
- Verificar que los modelos teóricos pueden ser llevados a la práctica, proporcionando de esta manera nuevas destrezas y competencias en el estudiante.
- Plantear desafíos de configuración y/o desarrollo utilizando la infraestructura virtual montada.
- Evaluar los conocimientos adquiridos, aplicando un cuestionario con una variedad de preguntas relacionadas con los procesos llevados a cabo en los laboratorios.

III. MODELOS DE CONFIANZA UTILIZANDO INFRAESTRUCTURA DE LLAVE PUBLICA

Esencialmente existen dos modelos para establecer confianza en las organizaciones que implementan infraestructuras de clave pública (PKI) [16], el modelo ***Certificación Jerárquica*** y el modelo ***Certificación Cruzada***.

En el modelo de Certificación Jerárquica [17] cada organización inicia su nivel de confianza estableciendo una AC raíz que autofirma (selfsign) su certificado (clave pública y atributos). Seguidamente, para hacer eficiente la administración de certificados, esta AC raíz, puede delegar la autoridad en otra AC denominada AC subordinada, logrando de esta manera el establecimiento de una cadena de certificación [18].

Es este modelo, cada miembro confía en el miembro que se encuentra en el nivel superior, hasta llegar al nivel que inicio la cadena de certificación, la AC raíz.

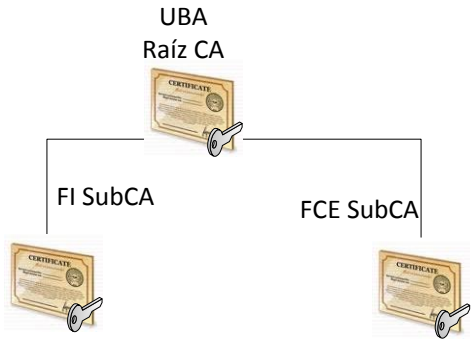


Ilustración 1 Modelo Certificación Jerárquica

Si cada organización tiene su propia jerarquía que incluye una AC raíz, al no tener un miembro en común (una AC raíz), las organizaciones no tienen confianza entre sí. Al intercambiar los certificados de la AC raíz y subordinada entre ellas, se establece una confianza absoluta entre ellas. En este modelo puede resultar difícil establecer políticas que limiten el nivel de confianza que se desea establecer.

Para regular el nivel de confianza de acuerdo a las necesidades de las organizaciones, se recurre al modelo de Certificación Cruzada [19] que consiste en que una organización por ejemplo la Facultad de Ciencias Económicas (FCE) proporcione a la Facultad de Ingeniería (FI) el certificado de la SubCA, esta última mediante el proceso descrito en la siguiente sección, genera un nuevo certificado que contiene todos los elementos que le permiten ejercer el control adecuado (granularidad) al momento de acceder los recursos de su par (confianza en un sentido).

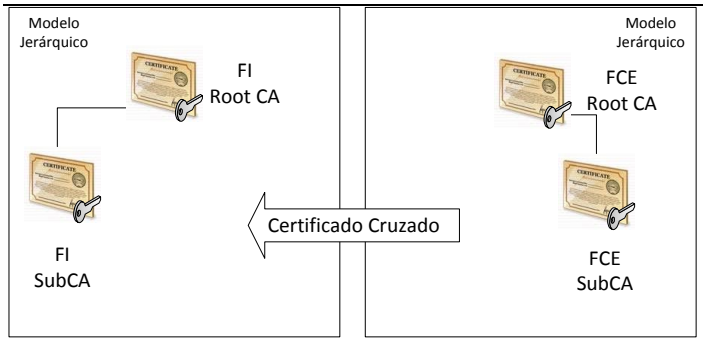


Ilustración 2 Modelo Certificación Cruzada.

IV. PROCESO DE CERTIFICACION CRUZADA

En esta sección se describen los pasos que los estudiante deben seguir para efectuar el proceso de Certificación Cruzada entre organizaciones [15]. Para facilitar la comprensión se proporciona el siguiente escenario hipotético: Los equipos de la Facultad de Ingeniería (FI) acceden mediante un navegador web a una aplicación de la Facultad de Ciencias Económicas (FCE) para consultar información estadística que le permite elaborar su presupuesto anualmente. Para minimizar riesgos relacionados con la seguridad y así evitar que el personal administrativo (de la FI) sea engañado (accediendo a otro sitio maliciosamente colocado) sin ser advertido. La FI ha determinado efectuar el proceso de certificación cruzada, por lo que efectúa los siguientes pasos en el servidor Windows Server 2008 que ejecuta el servicio de Active Directory Certificate Services y que a la vez contiene la AC FI SubCA

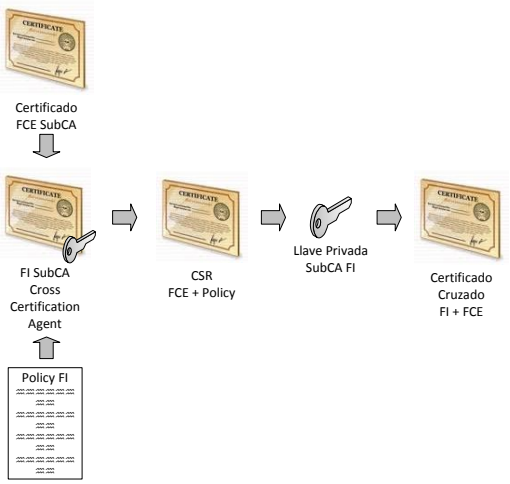


Ilustración 3 Proceso de emisión del certificado cruzado

Procedimiento seguido por el alumno:

- Desde una máquina de la FI comprueba que al acceder el servidor web de la FCE (https://websrv.fce.uba.ar) aparece el error de confianza del certificado.
- Construye la plantilla del Agente que genera la solicitud (Cross Certification Enrollment Agent) de certificado cruzado en el servidor Windows server 2008.
- Incorpora las plantillas Cross Certification Enrollment Agent y Cross Certificate Authority a la lista de plantillas disponibles para emisión de certificados.
- Genera el certificado del Agente utilizando la plantilla Cross Certification Enrollment Agent.
- Construye y parametriza el archivo de políticas de certificación (policy.inf) para que únicamente se confíe en el servidor web (https://websrv.fce.uba.ar).
- Copia el certificado de AC subordinada FCE SubCA en el servidor FI SubCA.
- Genera la solicitud del certificado (CSR) utilizando el comando certreq –policy. Esta solicitud contiene el certificado FCE SubCA junto con las restricciones establecidas en el archivo policy.inf.
- Solicita el nuevo certificado mediante la consola de la FI SubCA utilizando el CSR del paso anterior.
- Emite el certificado cruzado utilizando la llave privada de la Autoridad Certificante FI SubCA.
- Comprueba que en el certificado emitido se muestra el certificado de la FI SubCA como parte de la jerarquía.
- Distribuye el nuevo certificado en el repositorio de Autoridades Certificantes Intermedias de los equipos de la FI.
- Efectúa las pruebas correspondientes que consisten en ingresar al servidor web de la FCE desde un equipo de la FI. Comprueba que en esta ocasión no se presenta en el navegador alerta alguna en relación a la confianza del certificado de la FCE.
- En las propiedades del certificado cruzado comprueba que en la viñeta que corresponde a la ruta de certificación a las AC de la FI.

Efectuados los pasos anteriores, el estudiante debe comprobar el acceso satisfactorio a la aplicación estadística ubicada en el servidor https://websrv.fce.uba.ar (no se presenta ningún mensaje de advertencia con respecto a la confianza del certificado y al momento de revisar en la barra de direcciones, se

muestra el candado que indica el acceso a un sitio de confianza), pero cuando acceden a cualquier otro servidor de la FCE (que no se ha incluido en la política), se presenta el mensaje de advertencia indicando que no se confía en el sitio visitado.

V. PAUTAS DIDÁCTICAS

La principal pauta didáctica para el desarrollo del laboratorio, se refiere a que la tecnología se aprende mejor utilizándola y no sólo leyendo o recibiendo una descripción de cómo debe hacerse. Es por eso que uno de los objetivos fundamentales es el de implementar un caso real y es muy importante que sea en las horas de clase.

El hecho que los laboratorios se desarrollen en las horas de clase, permite que se puedan ir abordando y resolviendo las inquietudes del estudiante.

Para disminuir los tiempos de ejecución de los laboratorios, se proporcionan los entornos virtuales en VMWARE y se han probado en la versión Workstation y Player. En cuanto a la distribución de Linux, se ha utilizado una distribución Debian dela catedra, sin embargo se han hecho pruebas con Ubuntu 64 bits v.12.10

El estudiante debe completar un cuestionario al finalizar el laboratorio, persiguiendo dos objetivos, afianzar los conocimientos y que el docente efectúe la evaluación correspondiente.

Por último se plantea a los alumnos desafíos a resolver, por ejemplo, incorporar control de accesos a la aplicación de la FCE basado en atributos de los certificados, incorporación de verificación de estado por OCSP, establecimiento de SSL de dos vías entre módulos, etc.

VI. RESULTADOS

Las prácticas han sido productivas y permitieron afianzar los conocimientos brindados en las clases teóricas. Así mismo, de acuerdo a las encuestas, los estudiantes opinan que el escenario planteado y la asistencia brindada facilitan la comprensión y los encamina hacia un buen desarrollo de los laboratorios. Además, opinan que el tiempo que invirtieron en el desarrollo de los laboratorios aporta valor importante a sus conocimientos en relación a la seguridad de la información.

Algunos estudiantes que no han requerido ninguna asistencia, han desarrollado los laboratorios en un término de seis horas, esto incluye el tiempo requerido para instalación de servicios en el sistema operativo. Estudiantes con menos destrezas, han requerido con la ayuda del plantel docente de nueve horas.

VII. CONCLUSION

Mediante la práctica de los laboratorios, el estudiante adquiere destrezas y competencias que le ayudan a tener un mejor enfoque y a familiarizarse con los conceptos de certificados digitales que hoy día son utilizados ampliamente por las organizaciones.

Este laboratorio permite a la catedra trabajar el concepto de Confianza establecida entre organizaciones utilizando ambientes reales y heterogéneos como son los de Windows y Linux.

Dicho sistema fue usado y verificado con éxito en nuestra catedra, facilitando el proceso de aprendizaje de PKI. Hemos tenido una muy buena recepción del material por los alumnos quienes han sugerido numerosos cambios y mejoras. Es muy importante recalcar que el material permitió que los estudiantes desarrollen las configuraciones de los laboratorios en forma rápida y con buenos resultados.

REFERENCIAS

[1] K. Raina, PKI Security Solutions for the Enterprise, Indianapolis, Indiana: Wiley Publishing, Inc., 2003.

[2] R. A. Española, "Diccionario de la lengua española," Real Academia Española, [Online]. Available: http://www.rae.es/rae.html, http://www.rae.es/drae/srv/search?id=ttIyhpiT7DXX2p26VbYf. [Accessed 7 6 2013].

[3] DATALOSSdb, "DATALOSSdb," Open Security Foundation, 21 06 2013. [Online].

Available: http://datalossdb.org/incidents/10397-6-million-users-email-addresses-and-phone-numbers-exposed-due-to-a-bug. [Accessed 29 06 2013].

[4] Certisur, «Certisur,» [En línea]. Available: https://www.certisur.com/eventos-y-noticias/201207-Nuevas-Normativas .

[5] Certification Authority Browser Forum, "CA/Browser Forum," CA/Browser Forum, [Online]. Available: https://www.cabforum.org/forum.html. [Accessed 13 07 2013].

[6] R. Kuhn, V. C. Hu, T. Polk and S.-J. Chang, Introduction to Public Key Technology and the Federal PKI Infrastructure SP 800-32, National Institute of Standards and Technology, 2001, p. 15.

[7] Microsoft Corpotation, "Qualified subordination overview," Microsoft Corpotation, 2005 Enero 2005. [Online]. Available: http://technet.microsoft.com/en-us/library/cc786077(v=ws.10).aspx. [Accessed 14 07 2013].

[8] R. Moulds, Key Management For Dummies, Hoboken: Wiley, 2001.

[9] B. Komar, Windows Server 2008 PKI and Certificate Security, Redmond, Washington: Microsoft Press, 2008.

[10] E. p. d. I. 27001, "El portal de ISO 27001," [Online]. Available: http://www.iso27000.es/glosario.html. [Accessed 09 10 2013].

[11] G. Millan, "Infraestructuras de certificacion cruzada," *Boletin de RedIRIS,* vol. 71, no. Enero http://www.rediris.es/difusion/publicaciones/boletin/70-71/ponencia14.pdf, enero 2005.

[12] "OpenSSL PKI Tutorial," [Online]. Available: http://pki-tutorial.readthedocs.org/en/latest/simple/index.html. [Accessed 26 10 2012].

[13] "Debian Project," [Online]. Available: http://www.debian.org/.

[14] "Open SSL Project," [Online]. Available: http://www.openssl.org/.

[15] B. Komar, Windows Server 2008 PKI and Certificate Security, Microsoft Press, 2008.

[16] "Trust Models," Microsoft Corporation, [Online]. Available: http://msdn.microsoft.com/en-us/library/windows/desktop/bb540815(v=vs.85).aspx. [Accessed 26 10 2012].

[17] "Certificate Hierarchy," Microsoft Corporation, [Online]. Available: http://msdn.microsoft.com/en-

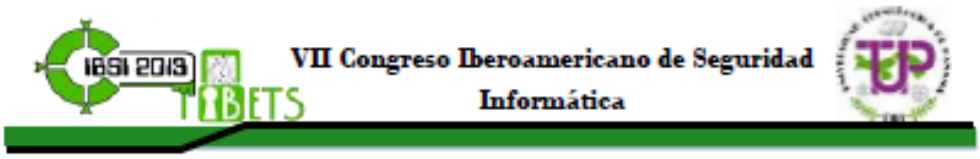
us/library/windows/desktop/bb931353(v=vs.85).aspx. [Accessed 26 10 2012].

[18] "Certificate Chain," Microsoft Corporation, [Online]. Available: http://msdn.microsoft.com/en-us/library/windows/desktop/bb540794(v=vs.85).aspx.

[19] "Cross Certification," Microsoft Corporation, [Online]. Available: http://msdn.microsoft.com/en-us/library/windows/desktop/bb540800(v=vs.85).aspx.

[20] Microsoft Corporation, "Developer Network," Microsoft Corporation, [Online]. Available: http://msdn.microsoft.com/en-us/library/ms524668(v=vs.90).aspx. [Accessed 15 06 2013].

Carta de aceptación VII Congreso Iberoamericano de Seguridad Informática



2 de Septiembre del 2013

CARTA DE ACEPTACIÓN
Estimados

Edy Milla, Hugo Pagola, Alberto Dams

Su trabajo: **"Laboratorio de confianza entre organizaciones utilizando certificación cruzada"**, ha sido aceptado para el **II Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información TIBETS 2013**, el cual se llevará a cabo del 29 al 31 de Octubre, en la Universidad Tecnológica de Panamá, República de Panamá.

Por favor consulte las instrucciones, el lugar y hora de su presentación en la página web del congreso: www.cibsi.utp.ac.pa

Saludos,

MSc. Glovana Garrido
Comité Organizador
VII Congreso Iberoamericano de Seguridad Informática CIBSI 2013 y
II Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información TIBETS 2013

www.cibsi.utp.ac.pa
Teléfono: 560-3616