INSTITUTO UNIVERSITARIO AERONÁUTICO

TRABAJO FINAL DE POSGRADO

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

APLICACIÓN DE FIRMA ELECTRÓNICA A PROCESOS DEL IUA

ALUMNO:

FERNANDO BOIERO- D.N.I. 27.880.277

TUTOR: MCS. ING. EDUARDO CASANOVAS

DICIEMBRE

2014

ÍNDICE TEMÁTICO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

01. INTRODUCCIÓN

La confianza es parte fundamental de cualquier comunicación, ya sea física o electrónica. En la comunicación física, lograr un nivel alto de confianza es simple ya que se puede identificar a la persona viéndola o bien, a través de algún mecanismo como su firma manuscrita. Sólo en ocasiones puntuales, por la necesidad de garantizar esta confianza, se necesita recurrir a una tercera parte que brinde certeza de su validez, como por ejemplo recurriendo a un escribano público para garantizar una firma hológrafa. Sin embargo, en el caso de comunicaciones electrónicas, confiar en otra entidad es más complicado. La identidad en las comunicaciones electrónicas puede resultar menos clara que en la vida real, y en este caso, para tener certeza siempre es necesario recurrir a una tercera parte de confianza para garantizar su validez.

Una Infraestructura de Clave Pública o Public Key Infrastructure (PKI) proporciona la seguridad y confianza del mundo real en el mundo electrónico. Dicha infraestructura contienen el software, hardware, políticas y mecanismos de seguridad necesarios que permiten garantizar la ejecución de operaciones criptográficas como el cifrado, la Firma Digital o el no repudio de operaciones electrónicas.

En este trabajo se describe la implementación de una PKI utilizada para brindar confianza a la comunicación de correos electrónicos utilizados en las comunicaciones del Instituto Universitario Aeronáutico (IUA) así como para ganar en seguridad en sus mensajes.

A continuación, se reseña brevemente el contenido de los capítulos que integran el trabajo:

- *Capítulo 02 - Objetivos y alcance del trabajo*: se describen los objetivos generales y específicos, como así también la delimitación del trabajo.
- *Capítulo 03 - Marco Teórico de Infraestructura de Clave Pública*: se brindan detalles de los componentes de una PKI y su funcionamiento.
- *Capítulo 04 - Marco Legal vigente para Firma Digital*: se explica la normativa legal vigente respecto de Firma Digital en la República Argentina.
- *Capítulo 05 - Estudio de alternativas de software PKI*: se plantean alternativas de implementación de PKI.
- *Capítulo 06 - Detalles del software a utilizar*: se determina la combinación de software a utilizar para brindar una solución completa de PKI.

- *Capítulo 07 - Hardware a utilizar para montar la PKI*: se menciona el equipamiento y recursos a utilizar para implementar la solución.
- *Capítulo 08 - Descripción del proceso a abordar con PKI*: se explica el proceso de negocio a abordar para aplicar la solución propuesta.
- *Capítulo 09 - Implementación de la solución*: se detallan los procedimientos de implementación de la solución.
- *Capítulo 10 - Demostración de uso*: se muestra la solución aplicada a un caso de uso.
- *Capítulo 11 - Conclusión*: se entregan las conclusiones del trabajo.
- *Capítulo 12 - Trabajos Futuros*: se plantean futuras líneas de investigación para continuar este trabajo.
- *Capítulo 13 - Referencias bibliográficas*: se vincula este trabajo con las fuentes de información utilizadas para consulta.
- *Capítulo 14 - Glosario*: se definen conceptos para facilitar la lectura del documento.

02. OBJETIVOS Y ALCANCE DEL TRABAJO

02.01. SITUACIÓN PROBLEMÁTICA

Actualmente, la mayoría de la documentacion del IUA se gestiona en persona, con formularios impresos o con e-mails sin Firma Digital. Esta forma de trabajo depende en gran medida de la confianza en cada funcionario, sin dejar debida trazabilidad documentada de las actividades y generando gran acumulación de papeles para soporte de los procesos.

02.02. OBJETO DE ESTUDIO

En el presente Trabajo Final se analizará el concepto, aplicación práctica y beneficios del montaje de una infraestructura de clave pública en la red interna del IUA, cómo puede ayudar a trazabilidad de los procesos, agregando a la vez, propiedades de Seguridad Informática en las comunicaciones internas.

02.03. OBJETIVOS

A continuación se detallan los objetivos del proyecto, describiendo brevemente los resultados esperados a su conclusión.

02.03.1. OBJETIVO GENERAL

Implementar una PKI funcional de código abierto, y mostrar los beneficios de seguridad en el intercambio de documentos utilizados en procesos internos del IUA.

02.03.2. OBJETIVOS ESPECÍFICOS

- Implementar una solución PKI funcional para brindar seguridad a las comunicaciones del IUA.
- Mostrar las ganancias de seguridad la solucion a implementar.
- Utilizar en todos los casos herramientas open-source para asegurar su mantenimiento a futuro.

02.04. DELIMITACIÓN DEL PROYECTO

El presente trabajo se circunscribe a la implementación de la Autoridad de Certificacion y la prueba de conceptos utilizando los certificados emitidos para la firma de correos electrónicos institucionales.

Como se define en el apartado 11, se buscará a futuro implementar mejoras y aplicar el objeto de este trabajo a otros procesos internos del Instituto.

03. MARCO TEÓRICO DE INFRAESTRUCTURA DE CLAVE PÚBLICA

Una PKI (Public Key Infrastructure o Infraestructura de Clave Pública) es una conjunción, no sólo de elementos de hardware y software, sino también de políticas y procedimientos de seguridad necesarios que permiten la ejecución de operaciones criptográficas como el cifrado, la Firma Digital o el no repudio de los mensajes electrónicos. Es común observar la banalización o simplificación del término PKI, siendo éste utilizado sólo para referirse al uso de algoritmos de clave pública en comunicaciones electrónicas. Este significado es incorrecto ya que no se requieren elementos propios de una PKI para usar algoritmos de clave pública.

En general, una PKI permite a dos partes disponer de confidencialidad, autenticación e integridad en las comunicaciones sin tener que compartir ninguna información de antemano.

La criptografía de clave pública o criptografía asimétrica se basa en la generación de 2 claves, una pública y una privada, donde la primera es entregada libremente y la segunda es mantenida en total aislamiento para que nadie más que su generador pueda accederla o conocerla. A su vez, igualmente vital es que los mecanismos criptográficos (algoritmos) garanticen que la generación de claves sea única, es decir, que la pareja de claves se pueda generar una única vez para asegurar que nadie más pueda obtener casualmente la misma pareja de claves.

Los algoritmos de clave pública (por ejemplo RSA **[01]**), se basan en que cada usuario utiliza un par de claves relacionadas matemáticamente, de tal forma que una de ellas descifra el cifrado que se realiza con la otra. Estos algoritmos tienen la propiedad adicional de que, conociendo una de las claves del par, es computacionalmente imposible deducir la otra. Una de estas claves, que debe permanecer siempre en secreto, se conoce como privada y la otra como pública. Estos algoritmos permiten realizar dos operaciones:

- ***Cifrado***: Un mensaje cifrado con la clave pública de un destinatario no puede ser descifrado por nadie excepto por el destinatario que está en posesión de la correspondiente clave privada. Este mecanismo proporciona confidencialidad.

- ***Firma digital***: Un mensaje cifrado con la clave privada del emisor puede ser descifrado por cualquiera que tenga la clave pública de dicho emisor, probando de esa manera que sólo ese emisor pudo cifrar el mensaje y que no ha sido modificado. La Firma Digital proporciona autenticación.

Para utilizar los algoritmos de clave pública, cada una de las dos entidades que desean intercambiar información deben disponer de un par de claves relacionadas matemáticamente: una privada, que sólo conoce su propietario y otra pública que debe ser conocida por cualquiera que desee comunicarse con él.
La fortaleza de los algoritmos de clave pública más utilizados, reside en la dificultad de factorizar números grandes ya que la generación de claves se basa en elegir dos números primos pseudoaleatorios **[02]**. En la figura siguiente se observa el esquema genérico de generación de claves para un usuario.

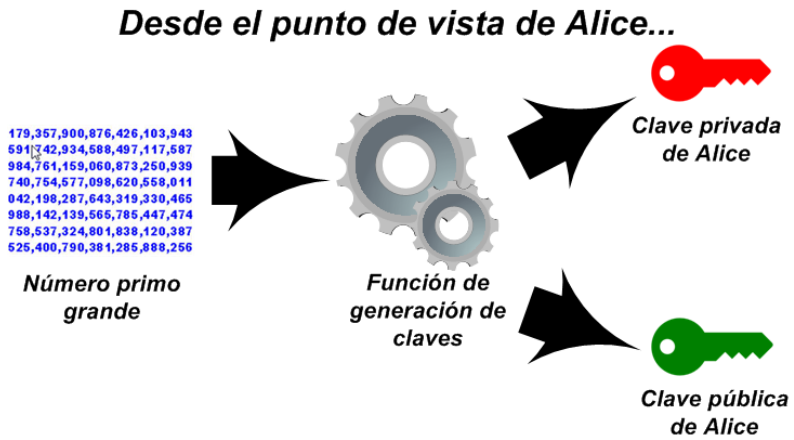

Figura N° 01 - Generación de claves pública y privada

Habiendo analizado la generación de claves, se describen 2 usos comunes en la infraestructura de clave pública.

03.01. CIFRADO DE DATOS

El cifrado de datos con algoritmos de clave pública se realiza de la siguiente forma: suponiendo que Bob desea enviarle un mensaje a Alice; Bob tomará el mensaje que desea enviar y lo cifrará con la clave pública de Alice; cuando Alice reciba el mensaje utilizará su clave privada para descifrarlo y leer el mensaje original que Bob deseaba enviarle. En la figura 02 siguiente se puede ver cómo funciona este mecanismo. Como Alice es la única que conoce su propia clave privada, sólo ella podrá descifrar el mensaje que le envía Bob. Mediante este procedimiento conseguimos realizar envío de datos con confidencialidad.
Debido a que los algoritmos asimétricos son bastante más lentos que los simétricos, lo que se hace realmente en este tipo de cifrados es:

1. Sortear una clave para un algoritmo de cifrado simétrico y cifrar el mensaje que se desea enviar.
2. Cifrar esta clave simétrica con la clave pública del destinatario y enviar el resultado junto con el cifrado anterior.

3. Cuando el destinatario reciba el mensaje descifrará la clave simétrica con su clave privada y la utilizará para descifrar el mensaje original.

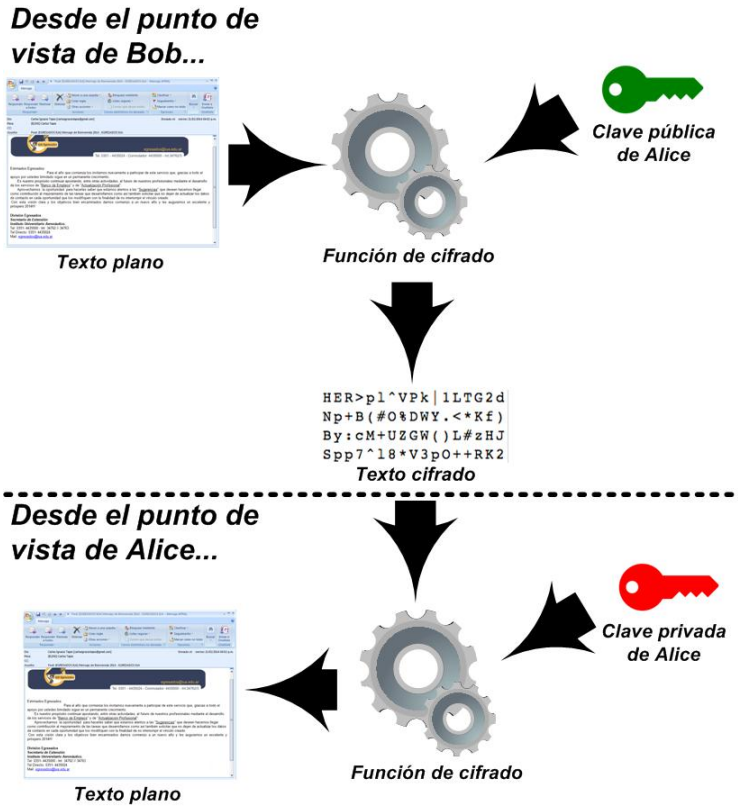

Figura N° 02 - Mecanismo de cifrado de datos

03.02. FIRMA DIGITAL

La Firma Digital es un procedimiento que permite simular la seguridad que proporciona la firma manuscrita convencional. Como se puede ver en la figura 03 siguiente, realizar una Firma Digital consiste en lo siguiente: planteando que Alice desea firmar digitalmente un contrato con Bob; Alice tomará el documento del contrato, lo cifrará con su clave privada y se lo enviará a Bob; Bob, que tiene la clave pública de Alice será capaz de descifrar el contenido del mensaje; como sólo Alice está en posesión de la clave privada, sólo ella pudo realizar el cifrado. Con este mecanismo se obtiene autenticación del emisor.

Como hemos visto en el punto anterior los algoritmos asimétricos son lentos por lo que si el mensaje que se desea firmar es muy grande, el proceso de firma y verificación puede llevar bastante tiempo. Debido a esto, lo que se hace en lugar de cifrar todo el mensaje es aplicar una “función hash” al mensaje original y cifrar el resultado.

Una función hash es una transformación que toma como entrada una secuencia de longitud arbitraria y devuelve una secuencia de longitud fija que se denomina valor hash

o resumen. El hash es un tipo de "huella digital" del documento original. Una función hash debe tener las siguientes propiedades:

- La función debe ser no invertible: dado un valor hash h debe ser computacionalmente imposible encontrar un valor m tal que h = hash(m).
- Dado un valor m1 debe ser difícil encontrar un valor distinto m2 tal que hash(m1) = hash(m2).
- Debe ser difícil encontrar dos valores m1 y m2 tal que hash(m1) = hash(m2).

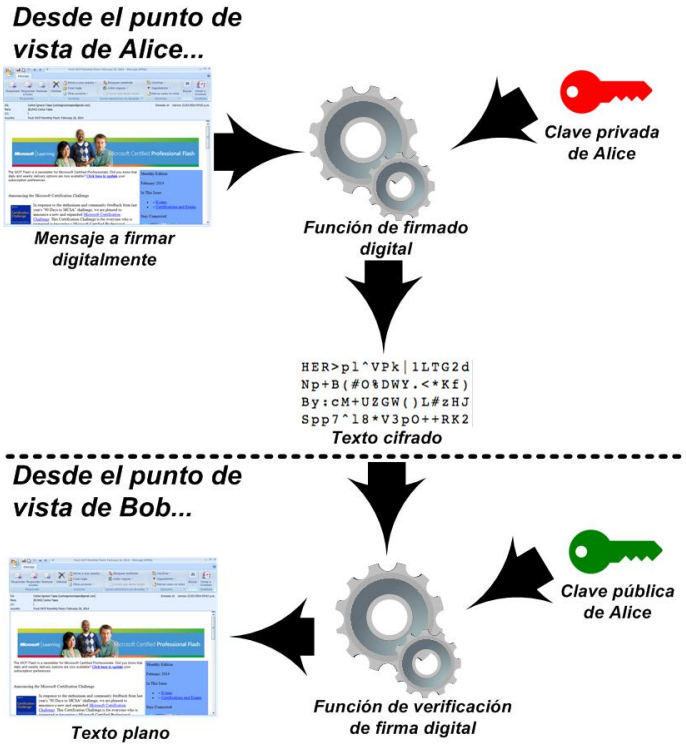

Figura N° 03 - Firma Digital y su verificación

Como se observa, un componente esencial de la PKI es el certificado digital. Cada certificado contiene la clave pública acompañada por otros parámetros relacionados con la clave. En el proceso de firmado digital se utiliza el certificado digital para constatar que la clave pública, necesaria para la verificación de la firma, pertenece al firmante. Adicionalmente, cada certificado contiene un conjunto de datos relevantes que son definidos en la recomendación ITU-TX.509 por medio de una estructura de certificado que actualmente se encuentra en su versión 3 **[03]**. En la sección siguiente se detallan sus características y atributos.

03.02.1. Certificados digitales

Los certificados digitales son los elementos basales de una infraestructura de clave pública. La finalidad de los certificados digitales es que mediante un documento firmado se pueda asociar la clave pública con una identidad inequívoca. Los datos que pueden ser detallados en la identidad son, por ejemplo, el nombre de la persona o de la organización, su país de procedencia, su dirección de e-mail, entre otros. Un certificado digital contiene los siguientes elementos fundamentales:

- La clave pública del sujeto.
- Los datos de identificación del sujeto.
- Firma Digital de una tercera parte que asegura que los dos elementos anteriores están relacionados.
- El sujeto asociado al certificado (persona o dispositivo).
- La Autoridad de Certificación (AC) que emite.
- La clave pública del par de claves.
- Los algoritmos usados en el certificado.
- Información de validez y determinación de la revocación.
- Distintas extensiones de X.509 versión 3.

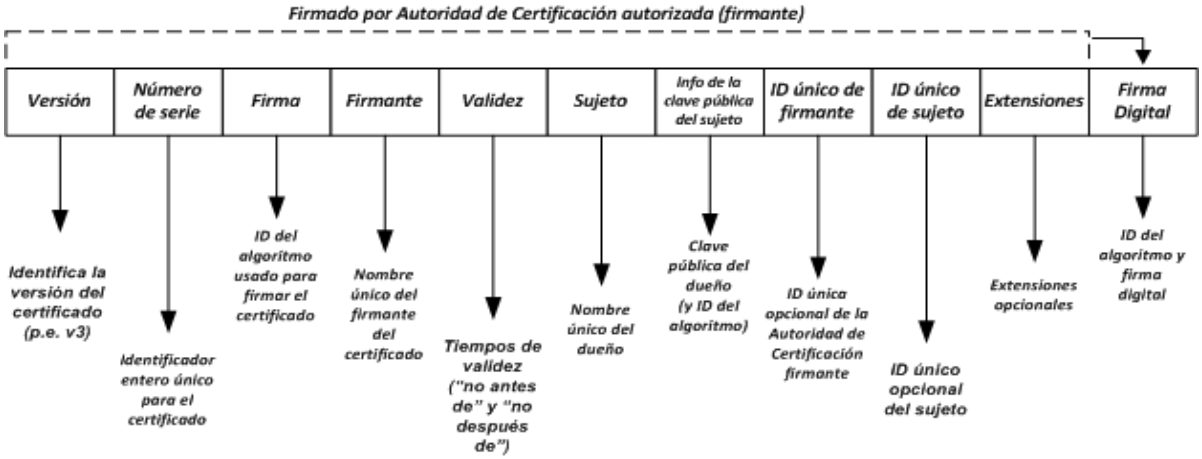

Figura N° 04 - Estructura de un certificado X.509 v3

En una PKI la firma del certificado la realiza una tercera parte confiable (Autoridad de Certificación), que es la que da fe acerca de la relación entre una identidad real y una electrónica. En otros sistemas, como los que siguen el estándar OpenPGP **[04]**, se utilizan los llamados esquemas de confianza, en los que son unos usuarios los que certifican la identidad de otros, en lugar de depender una única entidad confiable.

Respecto de extensiones, se destaca que proveen métodos para asociar atributos adicionales con usuario o claves públicas y para manejar la jerarquía de certificación. Es posible también definir extensiones privadas para completar información específica que sea de utilidad para los usuarios de los certificados. Dentro de un certificado, las extensiones se dividen en críticas y no críticas, actuando las primeras como causal de rechazo del certificado si no fueren reconocidas.

De acuerdo con X.509 v3 (RFC3280) **[05]**, las extensiones estándares son:

Nombre de la extensión	***Descripción***
Authority Key Identifier	Provee los medios para identificar la clave pública correspondiente a la clave privada usada para firmar el certificado.
Subject Key Identifier	Identifica la calve pública certificada por este certificado. Provee una forma de distinguir claves públicas si más de 1 está disponible para cierto nombre de sujeto.
Key Usage	Define el propósito de la clave contenida en el certificado. Usos posibles: • digitalSignature • nonRepudiation • keyEncipherment • dataEncipherment • keyAgreement • keyCertSign • cRLSign • encipherOnly • decipherOnly
Private Key Usage Period	Permite al generador del certificado especificar un período de validez diferente para la clave privada que para el certificado en sí.
Certificate Policies	Permiten informar los términos de las políticas bajo las cuales el certificado fue generado y los propósitos de su uso.
Policy Mappings	Se utiliza sólo en certificados de Autoridades de Certificación. Puede ser útil en el escenario de pares cruzados de certificados.
Subject Alternative Name	Permite adosar identidades adicionales al sujeto del certificado.
Issuer Alternative Names	Se utiliza para asociar la identidad en el formato usado en Internet con el generador del certificado.
Subject Directory Attributes	Permite detallar atributos de identificación del sujeto .
Basic Constraints	Indica si el sujeto del certificado es una Autoridad de Certificación
Name Constraints	Sólo se puede utilizar en certificados de Autoridades de Certificación. Define un espacio de nombres dentro del cual todos los nombres de los sujetos en certificados subsecuentes en la ruta de certificación deben localizarse.
Policy Constraints	Sólo se puede utilizar en certificados de Autoridades de Certificación. Restringe la validación de ruta de certificación a 2 vías.
Extended Key Usage	Da la posibilidad de ampliar los propósitos iniciales que se le dieron con la extensión Key Usage.
CRL Distribution Points	Define cómo se conseguirá la información de listas de certificados revocados.
Inhibit Any-Policy	Sólo se puede utilizar en certificados de Autoridades de Certificación. Con determinados valores, permite que no coincida con los criterios para determinadas políticas.
Freshest CRL (a.k.a. Delta CRL Distribution Point)	Provee un puntero a la lista de certificados revocados más actualizada posible.

Tabla N° 01 – Extensiones estándares de X.509 v3

Los tipos de archivo y por ende sus extensiones de archivo de certificados X.509 son:

- ***.CER***: Certificado codificado en CER **[06]**, algunas veces es una secuencia de certificados.
- ***.DER***: Certificado codificado en DER **[06]**.
- ***.PEM***: Certificado codificado en Base64, encerrado entre "-----BEGIN CERTIFICATE-----" y "-----END CERTIFICATE-----". Un archivo .PEM puede contener certificados o claves privadas, encerrados entre las líneas BEGIN/END apropiadas.
- ***.P7B***: Es un estándar para firmar o cifrar datos. Dado que el certificado es necesario para verificar datos firmados, es posible incluirlos en la estructura SignedData. Un archivo .P7C es simplemente una estructura SignedData, sin datos para firmar.
- ***.P7C***: Estructura PKCS#7 SignedData sin datos, sólo certificado(s) o CRL(s).
- ***.PFX***: Personal inFormation eXchange.
- ***.P12***: PKCS#12, puede contener certificado(s) (público) y claves privadas (protegido con clave). Evolucionó del estándar PFX y se usa para intercambiar objetos públicos y privados dentro de un archivo.

Es relevante destacar que los certificados digitales tienen un ciclo de vida con las siguientes etapas **[07]**, según los diferentes eventos o hitos que se sucedan durante su utilización: a) Revocación; b) Expiración; c) Renovación; d) Reemisión del par claves del usuario; e) Actualización de datos del certificado. Se esquematiza el ciclo de vida de los certificados digitales en el siguiente gráfico (figura 05):

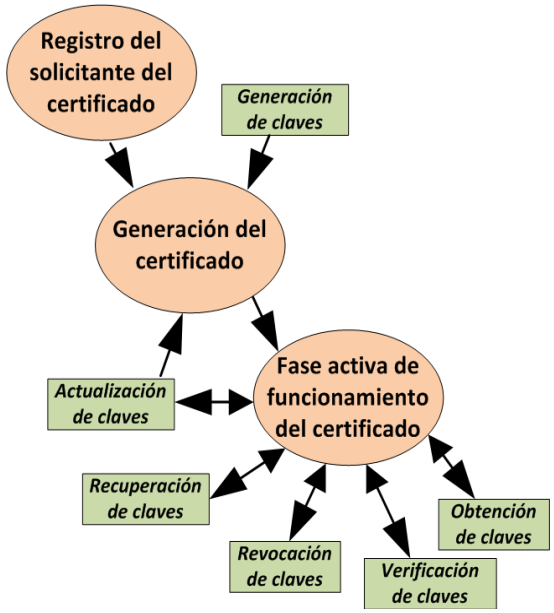

Figura N° 05 - Ciclo de vida de un certificado digital

03.03. PROPIEDADES DE SEGURIDAD QUE BRINDA UNA PKI

Las características de Seguridad de la Información que pueden obtenerse al implementar una infraestructura PKI son las que se enuncian a continuación:

- ***Confidencialidad***: Se refiere a la capacidad de proteger a una comunicación entre dos interlocutores para no ser interceptada ni interferida por una tercera persona que no forme parte de la comunicación. Para ello, la PKI utiliza mecanismos de cifrado que evitarían que individuos no autorizados se hagan de los mensajes.

- ***Autenticación***: Apunta a que se brinde acceso a una comunicación electrónica sólo a quienes se pueda corroborar su identidad y se pueda constatar su habilitación. En este caso, los certificados digitales y la estructura de confianza intrínseca a la PKI conforman una alternativa de autenticación a la tradicional presentación de credenciales (usuario/contraseña).

- ***Integridad***: Se necesario comprobar que la información enviada sea exactamente la misma que la que se reciba. El control apunta a garantizar que los datos no fueron alterados dentro del canal de comunicación. Adicionalmente, el control sirve para corroborar que 1 archivo se mantiene inalterado en el tiempo o en distintos medios de almacenamiento, garantizando que poseen en mismo contenido. A nivel técnico, este control es logrado a través de las funciones de hash que permiten efectuar comparaciones inequívocas de integridad de datos.

- ***No-repudio***: Esencialmente implica que los interlocutores no pueden negar haber enviado los mensajes que los muestren como remitentes. Esta propiedad hace que, ante algún problema entre las partes al haber intercambiado mensajes electrónicos, sea innegable evidencia presente dentro del sistema de comunicación que pueda ser utilizada para probar con suficiente certeza lo que realmente sucedió. Esto cobra especial importancia en operaciones financieras o trámites de índole legal cuyas consecuencias pueden ser de relevancia.

03.04. ELEMENTOS CONSTITUYENTES DE UNA PKI

03.04.1. Autoridad de Certificación

Como ya se mencionó previamente, el objetivo de una PKI es generar certificados digitales que asocien la identidad real de una persona, organización o incluso un dispositivo hardware con una clave pública. Una vez que una entidad dispone de un par de claves necesita que una tercera parte certifique y asocie ese par de claves con su identidad ante otras entidades. Esta tercera parte confiable en el mundo de las PKIs se denomina Autoridad de Certificación.

Una Autoridad de Certificación es un agente encargado de generar, custodiar y utilizar su propia identidad digital y de emitir los documentos digitales firmados que constituyen los certificados que emite. Un certificado digital es, en esencia, un documento digital firmado, cuya estructura es públicamente conocida y que incluye los datos verificados necesarios para poder afirmar lo que ese documento certifica.

Hasta este punto se disponían de mecanismos para realizar comunicaciones autenticadas y confidenciales, pero existía el problema de no tener certeza de que la clave pública de la otra entidad correspondiera a quién se creía, a menos que se verificara de manera externa. Ahora en lugar de tener la clave pública de otra entidad, disponemos de un certificado digital que asegura que dicha entidad es quien dice ser siempre y cuando confiemos en la Autoridad de Certificación que emitió su certificado.

Existen dos tipos de Autoridades de Certificación en función de quién firma su propio certificado:

- *Autoridad de Certificación Raíz*: Son aquellas que firman sus propios certificados con su clave privada. Este tipo de Autoridades de Certificación no disponen de una tercera parte confiable que aseguren que son quienes dicen ser. Es cada una de las entidades que vayan a utilizar el certificado de dicha autoridad la que debe decidir si confía o no en el mismo. La confianza o no en este tipo de autoridades suele venir dada por su reputación o conocimiento personal, por ejemplo, algunas grandes empresas dedicadas al negocio de las PKIs disponen de Autoridades de Certificación raíz generalmente aceptadas, e incluso instaladas como confiables por defecto en muchos navegadores web, sistemas operativos y demás software.

- *Autoridades de Certificación Subordinadas*: Este tipo de Autoridad de Certificación dispone de un certificado que no está firmado por sí mismas, sino por otra Autoridad de Certificación, ya sea raíz o no.

Con estos dos tipos de Autoridades de Certificación vemos que se pueden crear estructuras jerárquicas arborescentes en las que unas Autoridades de Certificación pueden firmar el certificado de otra autoridad o bien de un usuario final.

03.04.2. Autoridad de Registro

Este elemento de la PKI es el encargado de recibir las solicitudes de emisión de certificados para una determinada Autoridad de Certificación. Estos agentes deben controlar que todos los datos y documentos (digitales o no) que aporta una entidad son auténticos y que permiten identificar inequívocamente al solicitante del certificado.

Asimismo, tienen la responsabilidad de decidir si la solicitud es pertinente o no, y si puede emitirse el correspondiente certificado. Las Autoridades de Registro son una parte fundamental de una PKI ya que son las que comprueban la relación entre una clave pública y su propietario antes de que la Autoridad de Certificación la plasme en un certificado digital.

03.04.3. Dispositivos de usuario

Para que la utilización de los certificados sea practicable para los usuarios, se deben disponer herramientas software y/o hardware que actúen en su nombre y les permitan hacer uso de sus identidades digitales, más específicamente que sean capaces de:

- *Generar identidades digitales*: Los dispositivos deben contener un generador de secuencias aleatorias que les permitan generar el material de partida de las claves que constituyan una identidad digital, así como almacenarlas de forma segura.

- *Solicitar certificados digitales*: Una vez autorizado por la Autoridad de Registro, el dispositivo debe permitir solicitar a la Autoridad de Certificación un certificado digital asociado a un par de claves.

- *Realizar operaciones criptográficas*: Debe permitir firmar digitalmente o cifrar datos, con sus identidades digitales que son objetivos funcionales una PKI.

03.05. OBJETIVOS Y FINALIDADES DE UNA PKI

03.05.1. Verificación de certificados

Habiendo ya descrito los elementos de una PKI y la forma en que se generan los certificados digitales se debe analizar su modo de empleo. En este punto se sabe que en lugar de disponer simplemente de la clave pública de otra entidad, disponemos de su certificado.
Antes de utilizar un certificado es necesario verificar que está firmado por una Autoridad de Certificación confiable para el usuario. Para ello se deben realizar los siguientes pasos:

1. Si el certificado está auto firmado, es decir, la clave pública está firmada con la clave privada del mismo par de claves, entonces el usuario debe decidir si confía en el certificado o no.

2. Si el certificado está firmado por una Autoridad de Certificación raíz, el certificado será confiable si la Autoridad de Certificación que lo firmó es confiable para el usuario.

3. Si el certificado está firmado por una Autoridad de Certificación no raíz, entonces: si la Autoridad de Certificación es confiable el certificado lo será y si no se debe verificar el certificado de dicha autoridad desde el paso 2. A este procedimiento se le denomina verificación de la cadena de certificación.

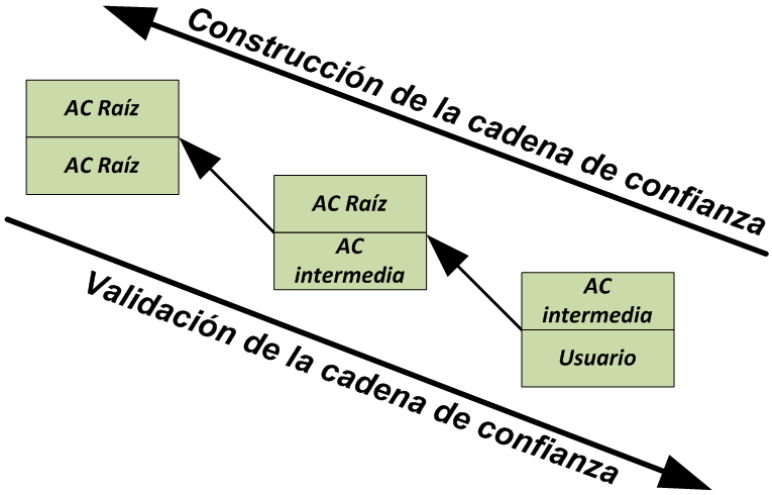

Figura N° 06 - Cadena de confianza de certificados

Viendo el procedimiento de verificación de certificados queda clara la estructura jerárquica de las PKIs.

03.05.2. Gestión de certificados

Precedentemente se detalló el proceso a seguir para solicitar un certificado digital, pero no es el único servicio que debe proporcionar una PKI. Los certificados digitales tienen una fecha de validez, que impone la Autoridad de Certificación, durante la que se compromete a certificar que un sujeto está vinculado a un par de claves. Una PKI debe disponer de protocolos para realizar otro tipo de trámites distintos de la solicitud de certificados entre los que se encuentran:

- *Revocación*: Un usuario o Autoridad de Certificación puede querer rescindir la asociación entre un individuo y su par de claves. Este proceso se conoce como

revocación de certificados. La necesidad de revocar un certificado puede deberse a varios factores, por ejemplo, un compromiso de seguridad de la clave privada por parte de un usuario o el cese de afiliación de un individuo dentro de la organización reflejada en su certificado.

- *Recertificación*: Los certificados digitales tienen fechas de validez que indican durante qué período un certificado es válido. Una vez finalizado el plazo de validez de un certificado, puede resultar útil que éste se pueda renovar durante un nuevo período de tiempo siempre que los datos de identificación del usuario y su par de claves sigan siendo válidos.

- *Renovación*: La renovación de un certificado consiste en solicitar un nuevo certificado con los mismos datos que el actual pero para un nuevo par de claves. Este procedimiento se realiza cuando un usuario desea cambiar el par de claves que utiliza, pero todos los datos de identificación siguen siendo válidos. La recertificación de certificados se puede ver como un caso particular de la renovación, donde el usuario mantiene el mismo par de claves.

La revocación de certificados debe ser un servicio obligatorio que debe proporcionar toda PKI, mientras que la recertificación y la renovación son opcionales. Algunas PKI pueden, además, obligar al usuario a volver a pasar por la Autoridad de Registro para volver a demostrar su identidad antes de permitir la realización de operaciones de recertificación y renovación. Todas las reglas que se deben cumplir para realizar estas operaciones deben ser mantenidas en la Política de Certificación que debe disponer toda Autoridad de Certificación y que debe estar disponible para todos sus usuarios.

03.05.3. Comprobación del estado de un certificado

En el punto precedente se analizó que algunos certificados pueden no ser válidos aunque estén dentro de su período de validez, ya que alguna circunstancia extraordinaria pudo provocar que se revocaran. Esto hace necesario disponer de mecanismos adicionales que permitan comprobar si un certificado ha sido revocado, y por tanto ya no es confiable lo que certifica, o no. La manera de acceder a este tipo de servicios suele venir definida en el propio certificado digital que se desea verificar.

Existen dos tipos de servicios que permiten realizar estas comprobaciones:

01) ***Servicios offline***: Las Autoridades de Certificación pueden poner a disposición de los usuarios, cada cierto tiempo, una lista con los certificados que están dentro de su período de validez pero que han sido revocados. Es tarea de los dispositivos de usuario obtener una copia actualizada de estas listas periódicamente para asegurarse de que un certificado no ha sido revocado antes de utilizarlo.

Para este tipo de servicio se utiliza el método de ***Certificate Revocation List (CRL)***, la cual es una lista con sello de tiempo, firmada por una Autoridad de Certificación, que contiene los números de serie de los certificados que han sido revocados y que puede estar en un repositorio público a disposición de los usuarios.

Cuando una aplicación requiere un certificado, además de comprobar la firma y la validez del mismo, debe controlar que el número de serie del certificado no esté presente en la última CRL emitida. Las listas de revocación de certificados se deben generar cada cierto tiempo, por ejemplo, cada hora o cada día. Cuando se revoca un certificado, éste deberá aparecer siempre en la siguiente CRL que se emita. Además, un certificado revocado deberá permanecer siempre en todas las CRLs siguientes hasta que se emita una CRL planificada para un momento posterior a la finalización de la validez del certificado. Esto evita el problema de que se revoque un certificado y que la próxima CRL se vaya a emitir después de la finalización de la validez del certificado; en este caso existiría un certificado revocado que nunca habría aparecido en una CRL. La mayor ventaja de este método de revocación es que las CRLs se pueden distribuir mediante los mismos medios que los certificados digitales, es decir, utilizando métodos de comunicación no confiables. La mayor limitación en el uso de CRLs es que la granularidad de la revocación en el tiempo está limitada por el período de publicación de las CRLs. Por ejemplo, si se realiza una revocación en este preciso momento, la información sobre esa revocación no estará disponible hasta que se publique la siguiente CRL, que puede ser dentro de una hora, un día o una semana dependiendo de la frecuencia de actualización de las CRLs.

02) ***Servicios online***: Algunas PKIs disponen de servicios en línea que permiten a un usuario consultar en cualquier momento el estado de un certificado que va a ser utilizado.

El protocolo de comprobación de estado de certificados que se utiliza para este caso es el ***Online Certificate Status Protocol (OCSP)***.

Este protocolo provee un método para determinar el estado de revocación de un certificado X.509 sin necesidad de utilizar CRLs. A diferencia de las CRLs, el protocolo OCSP proporciona información sobre el estado de revocación de un certificado en el momento actual. Los clientes OCSP realizan consultas a los servidores OCSP y aplazan el uso del certificado hasta que reciben una respuesta sobre el estado del mismo. Cuando un servidor OCSP recibe una solicitud deberá comprobar que está bien construida, que sea capaz de realizar el tipo de solicitud que le indica el cliente y que la información que necesita para procesar la solicitud es correcta. Todas las respuestas OCSP tienen que estar obligatoriamente firmadas digitalmente por la Autoridad de Certificación que emitió el certificado en cuestión o por una entidad confiable para el usuario para firmar respuestas OCSP. Este método es uno de los más utilizados en la actualidad para realizar consultas sobre el estado de los certificados. El diseño de

este protocolo se realizó basándose en la información disponible en las CRLs y con el objetivo de que ambos mecanismos fueran totalmente compatibles.

03.05.4. Publicación de certificados

Una vez que un usuario dispone de un certificado digital le surge la necesidad de compartirlo con otras entidades para poder comunicarse de manera segura con ellas. Suponiendo que un usuario desea enviar un mensaje cifrado a otro. Para ello el usuario debe disponer del certificado digital del destinatario. Con lo detallado hasta ahora el emisor debería solicitar al destinatario su certificado digital de manera convencional y después enviarle el mensaje cifrado que deseaba. Para evitar este inconveniente, las PKIs suelen proporcionar servicios de publicación de certificados, en los que los usuarios de una PKI, o incluso a veces cualquiera que lo necesite, pueda obtener los certificados emitidos para un usuario. Se reseñan a continuación 2 métodos:

01) ***Publicación Web***: Una forma simple de poner a disposición de los usuarios de una PKI los certificados de los demás miembros es utilizar un servidor Web de donde se puedan descargar mediante el protocolo http. El acceso a este servidor puede ser público (para cualquier persona) o privado, introduciendo algún mecanismo de control de acceso, por ejemplo algún método simple como autenticación mediante usuario/contraseña, o algo más complejo mediante previa identificación con el certificado del usuario.
Una vez que se tiene acceso a este repositorio se puede mostrar al usuario una lista con los certificados disponibles para que descargue el que necesite o bien disponer de una interfaz Web que permita realizar búsquedas.
Algunas soluciones existentes, como EJBCA, disponen de este mecanismo para realizar la publicación de certificados. EJBCA proporciona dos páginas web, una con enlaces directos a los certificados de las autoridades de certificación en diferentes formatos y otra con una caja de texto en la que se pueden realizar búsquedas de certificados por el número de serie o el DN (Distinguished Name).
Esta solución no es muy buena ya que no está estandarizada, sino que cada aplicación la implementa de acuerdo a sus necesidades y por tanto no se integra directamente con las aplicaciones en las que se suelen usar los certificados.

02) ***Lightweight Directory Access Protocol (LDAP)*:** Éste protocolo pertenece a la capa de Aplicación del modelo TCP/IP **[08]** y está basado en el estándar X.500 **[09]**, teniendo como función la realización de consultas y modificaciones sobre un servicio de directorio, entendiéndose éste último como un conjunto de objetos con atributos organizados en una jerarquía. Los servidores LDAP suelen utilizarse, para almacenar credenciales (usuarios y contraseñas) y también otro tipo de información como datos de contacto del usuario, certificados, etc. En resumen, el protocolo LDAP brinda acceso a un conjunto de información sobre una red y sus usuarios, cuya estructura de objetos y atributos es jerárquica y cuya raíz de la jerarquía se encuentra el “nodo raíz”.

04. MARCO LEGAL VIGENTE PARA FIRMA DIGITAL

Como se mencionó en la Introducción del presente trabajo, la Firma Digital consiste en un mecanismo por el cual se pueden rubricar documentos electrónicos de forma digital, de manera que el autor de esos datos pueda ser identificado inequívocamente, permitiendo que en el ámbito jurídico posea la misma validez que la firma hológrafa, inclusive existiendo casos donde la firma hológrafa fue falsificada, mientras que la Firma Digital no tiene hasta la fecha antecedentes de repudio. En este sentido, la Firma Digital garantiza mayor seguridad.

04.01. LEY DE FIRMA DIGITAL: / ANTECEDENTES

El 14 de noviembre de 2001, el Senado y la Cámara de Diputados de la Nación Argentina reunidos en Congreso, sancionaron la Ley 25506 (en adelante "la **Ley de Firma Digital**" **[10]**), incorporando al derecho argentino la Firma Digital.

Esta Ley define a la Firma Digital en su artículo segundo, como ***"resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La Firma Digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma."***

Conforme a la "**Ley de Firma Digital**", si un documento firmado digitalmente es verificado correctamente, se presume salvo prueba en contrario, que proviene del suscriptor del certificado asociado y que no fue modificado.

Además conforme lo establecido en la "**Ley de Firma Digital**", incorpora la posibilidad de otorgar actos y contratos, con pleno valor jurídico, mediante documentos digitales y firmarlos digitalmente. Se equipara la validez del soporte electrónico a los documentos manuscritos tradicionales exigidos en forma escrita, con la Firma Digital como modo para suscribirlos.

En su texto, la Ley en su artículo tercero, indica que cuando se requiera una firma manuscrita, esa exigencia también quedará satisfecha por una Firma Digital. Este principio es aplicable a los casos en que la Ley establece la obligación de firmar o prescribe consecuencias para su ausencia.

Para la actual Ley de "**Firma Digital**" existen dos maneras de realizar este proceso: 1) Usando certificados emitidos por un Certificador Licenciado y suscribiendo a sus políticas (a este proceso se lo denomina **Firma Digital)**; 2) La otra forma es realizar esta acción con certificados emitidos por un certificador no licenciado, suscribiendo a sus políticas, (**Firma Electrónica)**.

04.02. DECISIÓN ADMINISTRATIVA Nº 927 (30/10/2014)

Esta Decición Administrativa de la Jefatura de Gabinete de Ministros **[11]**, establece el marco normativo de Firma Digital aplicable al otorgamiento y revocación de las licencias a los certificadores que así lo soliciten, conforme a los requisitos y procedimientos establecidos en ella y sus Anexos.

Entre otros aspectos define la Infraestructura de Firma Digital de la República Argentina, estableciendo una Autoridad de Certificación Raíz y un sólo nivel de Autoridades de Certificación Subordinadas. Los Certificadores Licenciados actuales son los siguientes:

- *Estatales*:
  - Administración Federal de Ingresos Públicos (AFIP)
  - Administración Nacional de la Seguridad Social (ANSeS)
  - Oficina Nacional de Tecnologías de Información (ONTI)

- *Privados*:
  - ENCODE S.A.

04.03. APLICACIÓN DE FIRMA DIGITAL Y ELECTRÓNICA

Teniendo en cuenta los temas tratados, es necesario efectuar una distinción de conceptos y terminología utilizada para referirse al tema: es importante señalar que, aunque la legislación argentina emplea el término "Firma Digital" en forma equivalente al término "Firma Electrónica Avanzada" que se utiliza en la Unión Europea, o "Firma Electrónica" empleado en otros países como Brasil o Chile, la realidad es que para el régimen vigente los términos "Firma Digital" y "Firma Electrónica" no poseen el mismo significado **[12]**.

La diferencia radica en el valor probatorio atribuido a cada uno de ellos. Concretamente, en el caso de la "Firma Digital" existe una presunción "iuris tantum" en su favor; esto significa que si un documento firmado digitalmente es automáticamente verificado como correcto se presume salvo prueba en contrario por parte del demandante, que proviene del suscriptor del certificado asociado y que no fue modificado. Es decir, adquiere el carácter de documento público, a pesar de ser privado.

Por el contrario, en el caso de la "Firma Electrónica", se invierte la carga probatoria con respecto a la anterior. O sea que en caso de ser desconocida la firma, corresponde a quien invoca su autenticidad acreditar su validez.
Por ejemplo, si entre dos partes que celebran un contrato firmado digitalmente (no electrónicamente) y una de ellas alegase la invalidez de alguna de las dos firmas, le corresponde a ésta demostrar ante la Ley la invalidez de la misma. En caso de no tener la capacidad de demostrarlo, para la Ley argentina esa Firma Digital es válida.

Si en lugar de ello, las partes firmasen el contrato con firma electrónica, ante el mero alegato de una de ellas sobre la invalidez de alguna de las firmas, corresponde a la parte que clama por su validez demostrar ante la Ley la autenticidad de la misma. En caso de no tener la capacidad de demostrarlo, para la Ley argentina esa firma electrónica no es válida.

Por otra parte, para reconocer que un documento ha sido firmado digitalmente se requiere un certificado digital del firmante que haya sido emitido por un certificador licenciado en el marco de la Ley de Firma Digital (o sea que cuente con la aprobación del Ente Licenciante).

Es por esto que, si bien entendemos que en los ambientes técnicos se emplea habitualmente el término Firma Digital para hacer referencia al instrumento tecnológico, independientemente de su relevancia jurídica, es conveniente que todos los proveedores de servicios de certificación, divulgadores de tecnología, consultores, y demás actores involucrados empleen la denominación correcta según sea el caso, a fin de no generar confusión respecto a las características de la firma en cuestión.

05. ESTUDIO DE ALTERNATIVAS DE SOFTWARE PKI

En el rubro de software para montar una PKI existen actualmente una serie de alternativas con distintas características y capacidades. A continuación se describen algunas de las soluciones open-source que existen en el mercado, para posteriormente definir cuál será seleccionada para implementar en el ambiente de laboratorio del IUA.

05.01. OPENSSL

El proyecto OpenSSL **[13]** es un esfuerzo colaborativo para desarrollar un conjunto de herramientas de código abierto, robustas, de nivel comercial y con el mayor número de características disponibles que implementen protocolos para establecimiento de comunicaciones seguras, así como una biblioteca criptográfica de propósito general que pueda ser utilizada por cualquier software que requiera sus funciones. Este proyecto está formado por tres elementos:

a) Biblioteca que implementa los protocolos SSL y TLS.
b) Biblioteca criptográfica.
c) Aplicación de línea de comandos que permite utilizar los mecanismos implementados en las dos bibliotecas anteriores.

Si bien mediante la línea de comandos es posible construir una PKI funcional, resulta complejo ya que es necesario crear invocaciones al comando openssl con gran número de parámetros siendo la posibilidad de error muy alta a la hora de la implementación y de considerable dificultad su mantenimiento y modificación. Por este motivo, no es muy recomendable construir una PKI directamente con OpenSSL, sino más bien, puede ser utilizado como componente en el conjunto de la infraestructura.

05.02. EJBCA

Enterprise Java Bean Certificate Authority (EJBCA) **[14]** es un paquete de software que permite el montado de una infraestructura PKI completa y funcional. Se basa en tecnología J2EE que permite lograr la independencia de la plataforma (si bien los tests conducidos fueron hechos en Linux). EJBCA permite instalar una solución total para la infraestructura PKI de cualquier organización, implementando los siguientes componentes clave:

- Autoridad de Certificación (CertificateAuthority – CA).
- Autoridad de Validación (ValidationiAuthorrity).
- Respondedor OCSP (OCSSP Responder).

Tanto el acceso de administración como la interfaz de gestión de certificados se utilizan vía web, mediante navegador.

Como características destacables se pueden mencionar:

- Instalación y configuración simples.
- Manejo de múltiples CA y múltiples niveles de CA en simultáneo.
- Número ilimitado de CA raíces y Sub-CA.
- Soporte para hardware criptográfico.
- Soporta múltiples estándares criptográficos (X509, RSA, DSA, ECDSA, SHA-1, SHA-2, etc.)
- Soporte para protocolos de comprobación de estado de certificados.
- Almacena tanto los certificados como las listas de revocación en una base de datos SQL, directorio LDAP o en otras fuentes de datos.
- Íntegramente open-source certificada por la entidad Open Source Iniciative.

05.03. OPENCA PKI

El proyecto OpenCA **[15]** es un proyecto colaborativo cuyo objetivo es desarrollar una Autoridad de Certificación de código abierto recurriendo los algoritmos más utilizados por la comunidad. El proyecto OpenCA está basado en otros proyectos de código abierto como OpenLDAP, OpenSSL y el proyecto Apache.

Este software proporciona una interfaz web, a través del servidor Apache que permite realizar las operaciones proporcionadas por la Autoridad de Certificación: solicitudes, revocación, búsqueda de certificados. La configuración de las Autoridades de Certificación también se realiza mediante una interfaz web. La aplicación implementa protocolos de comprobación de estado de certificados, tanto online como offline, así como servicios de publicación de certificados.

05.04. ANÁLISIS DE SOFTWARE PKI COMERCIAL

A continuación se presenta una breve comparación de EJBCA con paquetes de software comerciales, mostrando que puede perfectamente competir con costos muy bajos o nulos.

Nombre de la solución PKI	*Costo de adquisición*	*Habilidad técnicas requeridas*	*Escalabilidad*	*Disponibilidad Soporte Técnico*	*Características de PKI avanzadas*
Symantec Managed PKI Service	Alto	Baja	Alta	Alta	Alta
Microsoft Windows Server 2012	Medio	Media	Alta	Media	Alta
Mac OS X	Bajo	Baja	Baja	Media	Baja
EJBCA	Bajo	Media	Alta	Alta	Alta

Tabla N° 02 - Comparación de soluciones PKI comerciales versus EJBCA

05.05. COMPARATIVA DE SOFTWARE PKI OPEN-SOURCE

Luego, teniendo en consideración las características de los 3 paquetes de software open-source presentados para montar una Infraestructura de Clave Pública, se plantean determinados criterios de evaluación, se las compara y finalmente se selecciona la solución a implementar. A continuación se presenta la tabla comparativa:

Criterio comparativo	*OpenSSL*	*EJBCA*	*OpenCA*
Cumplimiento con requerimientos de PKI funcional **(a)**	Medio	Alto	Alto
Dificultad de implementación **(b)**	Alta	Baja	Media
Calidad de la documentación **(c)**	Baja	Alta	Media
Afinidad de los implementadores con la solución **(d)**	Media	Alta	Baja
Lenguaje de programación principal **(e)**	C++	Java	Perl
Escalabilidad **(f)**	Baja	Alta	Media

Tabla N° 03 - Comparación de soluciones PKI open-source

(b) Respecto del cumplimiento con los requerimientos de una PKI funcional, se analizó si cada solución cuenta con las herramientas necesarias para montar la infraestructura en su totalidad, o requiere de otros productos o desarrollos adicionales. En esta categoría se destaca que tanto EJBCA como OpenCA son soluciones completas para el fin propuesto, no así OpenSSL.

(c) Para efectuar esta comparación se tomó la documentación publicada de cada solución, se descargó el software pertinente y se realizó un primer intento de implementación. Se observó que EJBCA quedó funcionando luego de seguir mínimas instrucciones, mientras que OpenCA presentó ciertas dificultades. OpenSSL calificó como la opción más dificultosa para implementar una PKI.

(d) A lo largo de la investigación, fue posible constatar que la documentación de EJBCA es adecuada para implementar la PKI, sin necesidad de búsqueda de mayor información. Para OpenCA fue necesario consultar mayor cantidad de información, y para OpenSSL se dificultó encontrar documentación clara para conseguir los objetivos del presente trabajo.

(e) Teniendo en cuenta las experiencias previas de los investigadores con EJBCA, dicha solución resultó más familiar que OpenCA y que OpenSSL.

(f) Teniendo en cuenta la afinidad de los investigadores con los lenguajes de programación C++ y Java, se prioriza EJBCA y OpenSSL por sobre OpenCA.

(g) EJBCA fue concebido independiente de la plataforma y completamente montable en clusters, favoreciendo fuertemente la escalabilidad en relación a OpenCA y OpenSSL.

Teniendo en cuenta los criterios de comparación analizados entre las distintas soluciones propuestas para montar una PKI, para implementar el ambiente de laboratorio se optó por EJBCA. Si bien OpenCA también tiene las funcionalidades necesarias para lograr los objetivos propuestos, EJBCA resultó más sencillo de instalar y utilizar, lo que permite concentrar los esfuerzos en mantener la PKI sin salidas de línea imprevistas y generar el cuerpo documental necesario para la implantación de la PKI en el IUA.

06. DETALLES DEL SOFTWARE A UTILIZAR

Teniendo en cuenta los análisis llevados adelante en los puntos anteriores, se concluye como la mejor alternativa, para la infraestructura de PKI a EJBCA.

Con EJBCA se pretende montar la infraestructura de PKI completa para el IUA, con todas sus funcionalidades básicas operativas, permitiendo la Firma Digital de documentos y correos electronicos.

Esta tecnología aplicada a un ambiente de laboratorio donde se instalará con una arquitectura simplificada como se muestra a continuación en la figura 08:

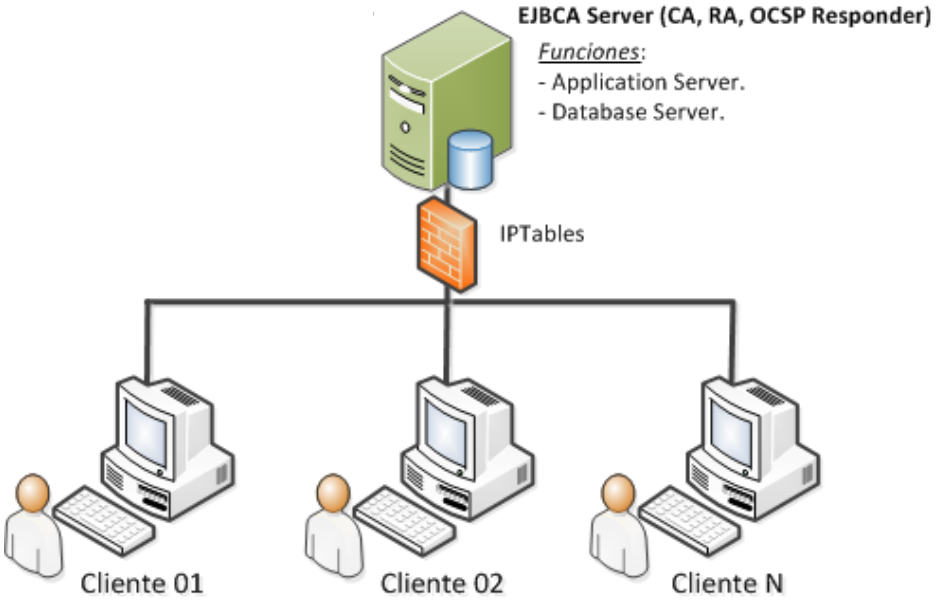

Figura N° 07 - Arquitectura simplificada de implementación de EJBCA

07. HARDWARE A UTILIZAR PARA MONTAR LA PKI

La siguiente tabla muestra las características del hardware físico que dispone el equipo a utilizar para el ambiente de laboratorio que es el contendrá las 2 virtual machines que sustentan la arquitectura conjunta de EJBCA y Alfresco.

Componentes de hardware físico disponible	
CPU	Intel Core i7 2.2 GHz (2
RAM	8 GB
Pagefile	8GB
Disco duro	1TB
Sistema Operativo host	Mac OS X

Tabla N° 04 - Componentes de hardware del equipo físico

A continuación se muestran los recursos virtuales que se utilizarán del hardware físico disponible en el equipo de pruebas, efectuando la virtualización con VMWare ESXi 5.5.0 (más detalles en Anexo IV):

01) Hardware virtual necesario para EJBCA:

Componentes virtualizados	Asignación de recursos físicos
VCPU	Intel Core i7 2.2 GHz (1 core)
VRAM	2GB
VHDD	20GB (SATA-VDI)

Tabla N° 05 - Hardware virtual para EJBCA

Tabla resumen de direccionamiento IP de cada Virtual Machine y sus hostnames:

La tabla siguiente muestra las configuraciones de direccionamiento IP que se dispusieron para cada virtual machine a los efectos de conformar la arquitectura de laboratorio dispuesta y que tengan conectividad para servir a su propósito.

Virtual Machine	*Dirección IP*	*Default Gateway*	*DNS Primario*	*Hostname*
VM1	192.168.1.220/24	192.168.1.1	192.168.1.221	AC01

Tabla N° 07 - Direccionamiento IP virtual

08. IMPLEMENTACIÓN DE LA SOLUCIÓN

Para implementar la solución se instalo y parametrizo la máquina virtual según se detalla en el apartado Anexos.

08.01. DESPLIEGUE DE EJBCA (VM01)

Una vez instalada y configurada la máquina virtual VM01 como se detalla en el Anexo I, se describe paso a paso la instalación del conjunto de soluciones PKI que trae la herramienta EJBCA y con la configuración inicial necesaria para poder emitir los certificados de Alumno, Docente y Empleado. Esta configuración describe los perfiles de certificados que se emitirán para las entidades finales. Para la correcta integración con el módulo de firma elegido para Alfresco los certificados serán emitidos con el formato PKCS#12. Éste contiene el certificado (público) y claves privadas, todo ello protegido por un pin (con clave).

Una vez aceptado por el Operador de la AR la emisión del certificado se termina una vez que le llega un correo al suscriptor con la URL para su generación y descarga. Cabe destacar que en ese mismo instante se genera el archivo p12 en memoria y lo entrega por parámetros para que lo descargue el suscriptor, ya que los mismos por cuestiones de seguridad no son almacenados en el servidor.

09. DEMOSTRACIÓN DE USO

En primer lugar tenemos que emitir los certificados para cada usuario del sistema que deba firmar electrónicamente. Para probar el concepto se van a emitir certificados de dos perfiles:

A. Docente.
B. Empleado

Los pasos para la Solicitud del certificado son los siguientes:

A. El usuario se acerca a la Autoridad de Registro solicitando se le extienda un certificado con la documentación que acredite su identidad y rol.
B. El oficial de registro constata que la documentación presentada sea la correcta y se corresponda con el solicitante.
C. Una vez constatada la documentación el oficial de registro accede al sitio web del EJBCA con su certificado instalado en su terminal colocando el pin asignado.
D. El sistema muestra el menú con las opciones autorizadas e ingresa a las opciones de la autoridad de registro, selección "Add End Entity" completa los datos según la documentación presentada y le hace cargar al usuario su password.

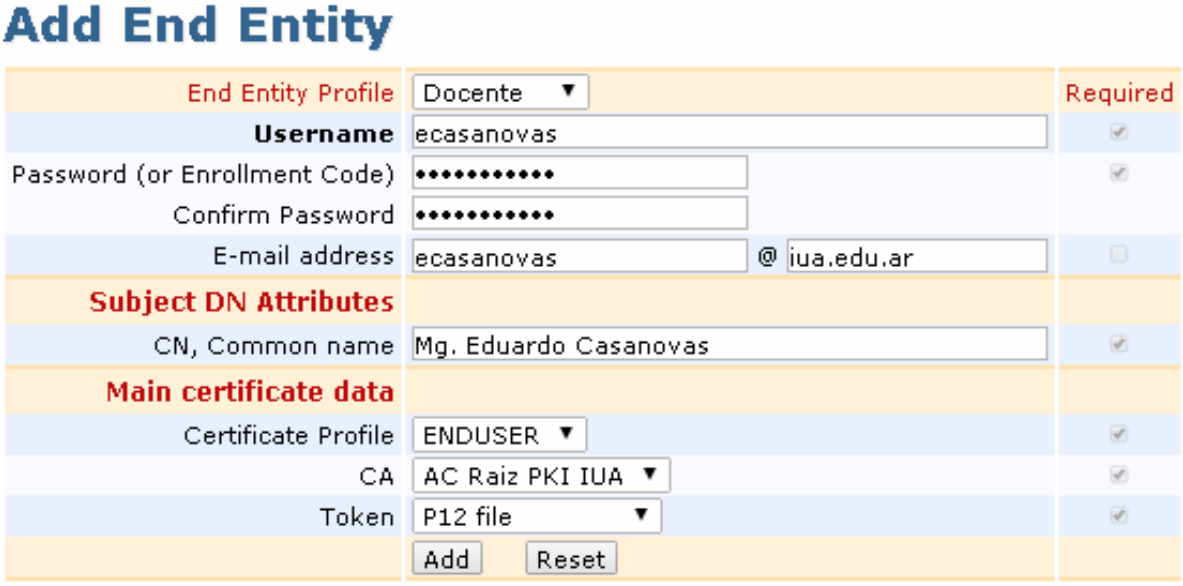

Figura N° 8 - Agregado de entidad en EJBCA

E. El usuario se retira y desde su terminal accede a la web publica del EJBCA con su usuario y password (https://ac01.pki.iua.edu/ejbca)

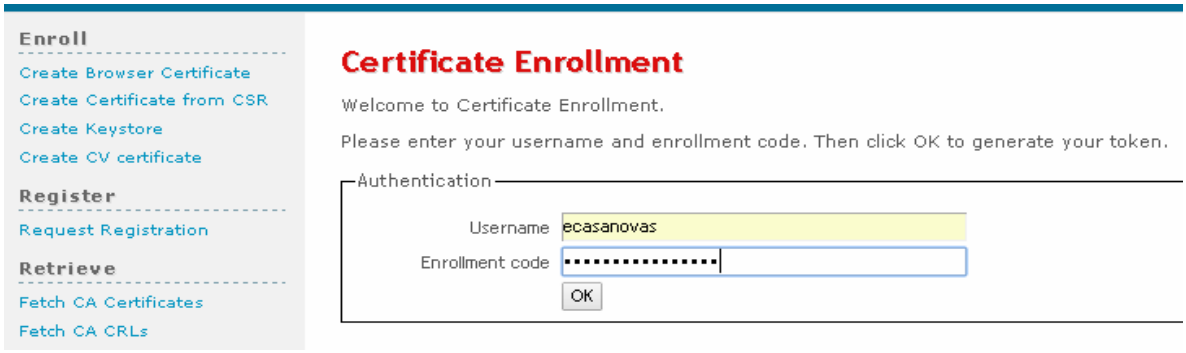

Figura N° 9 - Acceso de usuario a la interfaz web de EJBCA

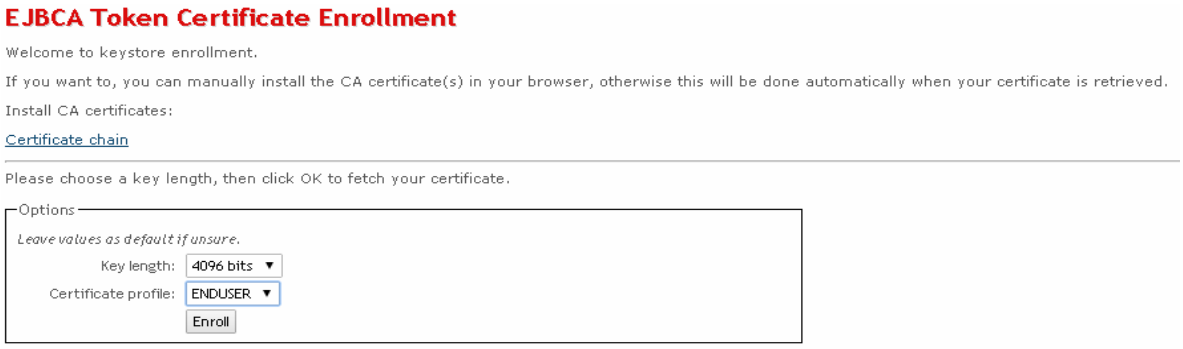

Figura N° 10 - Configuración del certificado a emitir en EJBCA

Figura N° 11 - Generación del certificado del usuario en EJBCA

Con el certificado generado y descargado en su terminal el usuario procede a instalarlo en el almacen de claves del sistema operativo.
A este procedimiento lo debe realizar cada usuario que necesite firmar digitalmente desde su terminal. A continuación se describen los pasos de un ejemplo e aplicación de Firma a un documento intercambiado.
El documento a firmar en este caso es en formato PDF. Se lo abre con el lector de PDF en este caso Acrobat Reader versión 11 o superior y se selecciona el icono Firmar en la barra de herramientas para abrir el panel Firmar o haciendo clic en el panel Firmar.

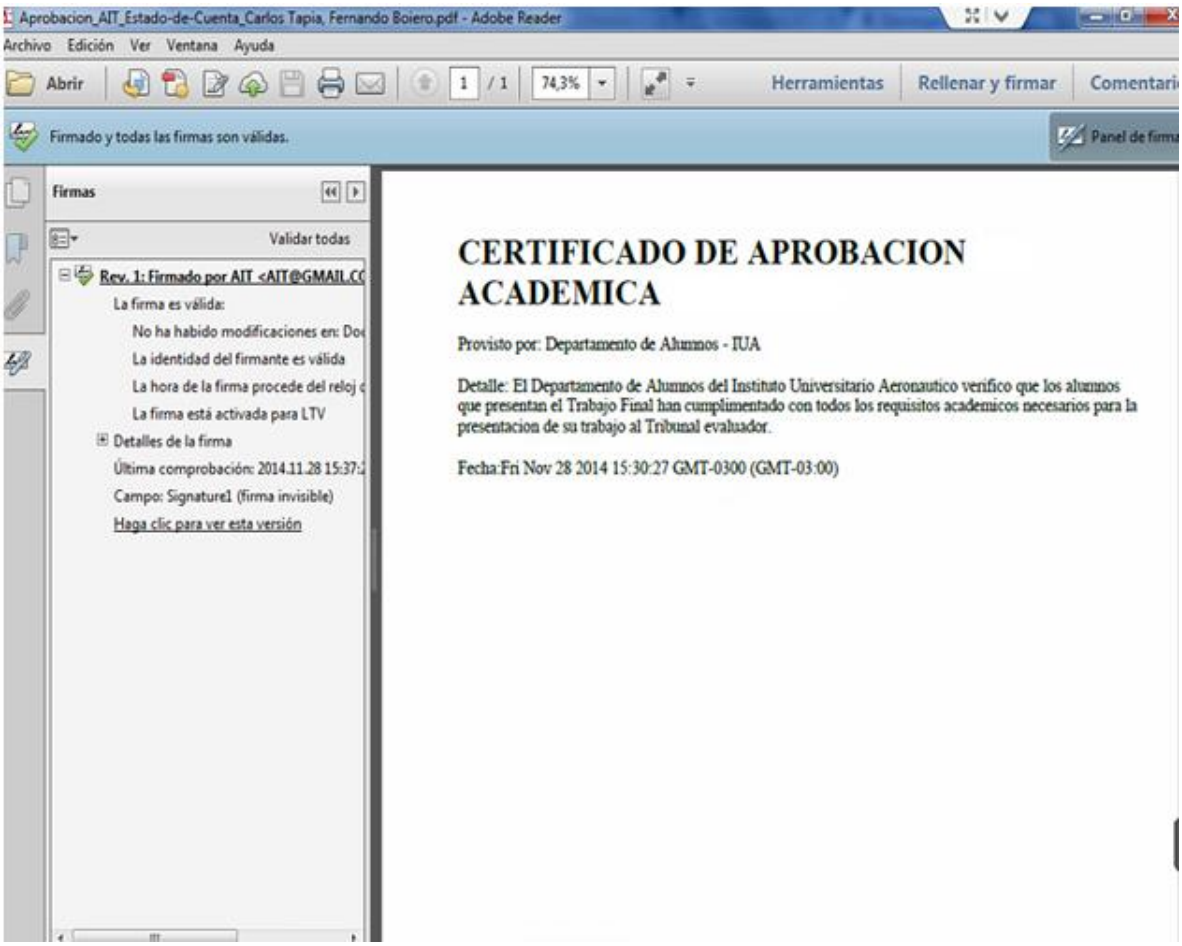

Figura N° 12 – Documento Firmado

10. CONCLUSIÓN

El presente trabajo mostró como es posible brindar seguridad a los procesos mediante la Firma Electrónica implementando una PKI.

En este documento se detalló cómo aplicando Firma Electrónica en reemplazo de la firma hológrafa en un proceso de IUA, se introdujeron mejoras en el flujo de información en la seguridad de cada etapa.

Para alcanzar este propósito se realizo una investigacion que nos llevo a la selección de las herramientas open-source que mejor se ajustaron a los requerimientos. Esta herramienta fue EJBCA para la solución de PKI.
De esta manera fue posible aplicar los distintos conocimientos adquiridos a lo largo de las materias de la Especialización, mostrando en la práctica las mejoras de seguridad y trazabilidad dadas a partir de la inclusión de las estas tecnologías y plataformas que garantizan el cumplimiento de los principios esenciales de la Seguridad de la Información: confidencialidad, integridad y disponibilidad.

El trabajo desarrollado es adaptable a muchos ámbitos, y puede ser de interés para muchas entidades y compañías que actualmente llevan a cabo sus procesos de manera manual o mixta, especialmente aquellas que cuenten con filiales o surcusales disperas geográficamente, o que necesiten una forma segura de acreditar sus transacciones electrónicas a un actor determinado. En este caso, el proyecto cobra mayor potencial teniendo en cuenta las distancias geográficas cubiertas por el IUA y sus centros académicos a lo largo del país y Uruguay, obervando gran aplicabilidad y expansión hacia futuro.

11. TRABAJOS FUTUROS

Ya habiendo realizado una implementación inicial de la PKI y Alfresco, los pasos a seguir que posibilitarían que el presente proyecto perdure en el tiempo y siga sustentable, son:

- Incorporación gradual de más procesos internos del IUA para utilizar estas tecnologías, desplazando la utilización del teléfono y el e-mail.

- Incremento en la documentación de los procesos, para facilitar la adaptación de los usuarios a los mismos.

- Lograr apoyo de las máximas autoridades del IUA para difundir la utilización de estas tecnologías entre los usuarios.

- Organizar reuniones de capacitación con los usuarios para entrenarlos en la utilización de las herramientas y explicar los fundamentos y beneficios.

- Impulsar o participar en el desarrollo de nuevas herramientas de software que funcionen en la arquitectura propuesta.

- Formalización de la Autoridad de Certificación del IUA a través de la confección, aprobación y publicación de los siguientes documentos:
  - Formulario de Adhesión a la Politica Única de Certificación
  - Política Única de Certificación.
  - Acuerdo tipo con Suscriptores.
  - Términos y Condiciones tipo con Terceros Usuarios.
  - Política de Privacidad del Certificador.
  - Manual de Procedimientos de Certificación.
  - Plan de Cese de Actividades.
  - Plan de Seguridad (política y procedimientos de seguridad).
  - Plan de Continuidad de las Operaciones.
  - Descripción de la plataforma tecnológica.
  - Descripción de los servicios brindados.

- Establecer convenios con otras universidades o estamentos del Estado para expandir el uso de PKI.

- Impulsar un convenio con la ONTI para obtener el status de Autoridad de Registro y emitir certificados bajo la AC – ONTI para obtener Firma Digital en procesos que necesiten este valor probatorio.

12. REFERENCIAS BIBLIOGRÁFICAS

[01] León, Jeffrey, apunte "RSA", asignatura "Codes and Cryptography", DMS, Univ. of Illinois at Chicago, 2008
http://homepages.math.uic.edu/~leon/mcs425-s08/handouts/RSA.pdf
Fecha de consulta: Mayo 2014

[02] Agustín, artículo "Entender RSA", Foro Técnico, Kriptópolis - Criptografía y Seguridad, 2012
http://www.kriptopolis.com/entender-rsa
Fecha de consulta: Marzo 2014

[03] International Telecommunication Union, "ITU-TX.509 Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks", Telecomm Standardization Sector of ITU, 2012
http://www.itu.int/rec/T-REC-X.509-201210-I/es
Fecha de consulta: Mayo 2014

[04] The Internet Engineering Task Force (IETF®) - OpenPGP Message Format - RFC4880, 2007
http://www.ietf.org/rfc/rfc4880.txt
Fecha de consulta: Septiembre 2014

[05] The Internet Engineering Task Force (IETF®) - Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile - RFC3280, 2002
http://www.ietf.org/rfc/rfc3280.txt
Fecha de consulta: Septiembre 2014

[06] International Telecommunication Union, "Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", Telecomm Standardization Sector of ITU, 2009
http://www.itu.int/rec/T-REC-X.690-200811-I/es
Fecha de consulta: Junio 2014

[07] Sriram Ranganathan, Sans Institute, "Key and Certificate Management in Public Key Infrastructure Technology", 2001
http://www.sans.org/reading-room/whitepapers/vpns/key-certificate-management-public-key-infrastructure-technology-735
Fecha de consulta: Junio 2014

[08] The Internet Engineering Task Force (IETF®) - A TCP/IP Tutorial, 1991
http://tools.ietf.org/rfc/rfc1180.txt
Fecha de consulta: Septiembre 2014

[09] International Telecommunication Union, "X.500: Tecnología de la información - Interconexión de sistemas abiertos - El directorio: Visión de conjunto de conceptos, modelos y servicios", Telecomm Standardization Sector of ITU, 2012
http://www.itu.int/rec/T-REC-X.500-201210-I/es
Fecha de consulta: Agosto 2014

[10] Congreso de la Nación Argentina, Ley Nacional, Ley de Firma Digital, 2001
http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70749/norma.htm
Fecha de consulta: Noviembre 2014

[11] Presidencia de la Nación Argentina, Jefatura de Gabinete de Ministros, Decisión Administrativa 927/2014, 2014
http://www.infoleg.gov.ar/infolegInternet/anexos/235000-239999/237642/norma.htm
Fecha de consulta: Noviembre 2014

[12] Gonzalez, José Luis, BDO Bercher Argentina para iProfesional, "Qué diferencia a la firma digital de la electrónica", 2007
http://www.iprofesional.com/notas/49143-Qu-diferencia-a-la-firma-digital-de-la-electrnica?page_y=0
Fecha de consulta: Noviembre 2014

[13] OpenSSL Project Wiki, OpenSSL Overview, 2013
http://wiki.openssl.org/index.php/OpenSSL_Overview
Fecha de consulta: Abril 2014

[14] Primekey, EJBCA PKI CA, EJBCA Wiki, 2014
http://wiki.ejbca.org/
Fecha de consulta: Abril 2014

[15] OpenCA Labs, Documentation, OpenCA PKI Wiki, 2014.
https://pki.openca.org/wiki/index.php/OpenCA_PKI
Fecha de consulta: Abril 2014

[16] Warren V, Blogspot, "Installing EJBCA 6.1.1 and Jboss on CentOS 6.5", 2014
http://ejbcacentos.blogspot.com.ar
Fecha de consulta: Julio 2014

[17] Majic, Branko, "Setting-up EJBCA as Certification Authority", Free Software X.509 Cookbook, 2010
http://majic.rs/book/free-software-x509-cookbook/setting-up-ejbca-as-certification-authority
Fecha de consulta: Julio 2014

[18] Osorio, Juan, "Evaluación de la herramienta EJBCA para un Prestador de Servicios de Certificación", Univ. Politécnica de Cataluña, 2008
https://upcommons.upc.edu/pfc/bitstream/2099.1/6100/1/Memoria_final_Juan_Alor.pdf
Fecha de consulta: Agosto 2014

13. GLOSARIO

- ***C++:*** es un lenguaje de programación diseñado a mediados de los años 1980 por Bjarne Stroustrup. La intención de su creación fue el extender al exitoso lenguaje de programación C con mecanismos que permitan la manipulación de objetos. En ese sentido, desde el punto de vista de los lenguajes orientados a objetos, el C++ es un lenguaje híbrido.

- ***DSA:*** (Digital Signature Algorithm, en español Algoritmo de Firma digital) es un estándar del Gobierno Federal de los Estados Unidos de América o FIPS para firmas digitales. Fue un Algoritmo propuesto por el Instituto Nacional de Normas y Tecnología de los Estados Unidos para su uso en su Estándar de Firma Digital(DSS), especificado en el FIPS 186.

- ***ECDSA:*** Elliptic Curve Digital Signature Algorithm es una modificación del algoritmo DSA que emplea operaciones sobre puntos de curvas elípticas en lugar de las exponenciaciones que usa DSA (problema del logaritmo discreto). La principal ventaja de este esquema es que requiere números de tamaños menores para brindar la misma seguridad que DSA o RSA.

- **Eclipse**: es un programa informático compuesto por un conjunto de herramientas de programación de código abierto multiplataforma para desarrollar lo que el proyecto llama "Aplicaciones de Cliente Enriquecido", opuesto a las aplicaciones "Cliente-liviano" basadas en navegadores. Esta plataforma, típicamente ha sido usada para desarrollar entornos de desarrollo integrados (del inglés IDE), como el IDE de Java llamado Java Development Toolkit (JDT) y el compilador (ECJ) que se entrega como parte de Eclipse (y que son usados también para desarrollar el mismo Eclipse).

- ***FIPS:*** Federal Information Processing Standards (FIPS, en español Estándares Federales de Procesamiento de la Información) son estándares anunciados públicamente desarrollados por el gobierno de los Estados Unidos para la utilización por parte de todas las agencias del gobierno no militares y por los contratistas del gobierno. Muchos estándares FIPS son versiones modificadas de los estándares usados en las comunidades más amplias (ANSI, IEEE, ISO, etc.).

- ***Firma Holografa:*** Una firma hológrafa, es una firma de puño y letra. Así cuando se habla de testamento hológrafo se dice q el mismo fue otorgado de puño y letra por el testador.

- ***Java:*** es un lenguaje de programación de propósito general, concurrente, orientado a objetos que fue diseñado específicamente para tener tan pocas dependencias de implementación como fuera posible. Su intención es permitir que los desarrolladores de aplicaciones escriban el programa una vez y lo ejecuten en cualquier dispositivo (conocido en inglés como WORA, o "write once, run anywhere"), lo que quiere decir que el código que es ejecutado en una plataforma no tiene que ser recompilado para correr en otra. Java es, a partir de 2012, uno de los lenguajes de programación más populares en uso, particularmente para aplicaciones de cliente-servidor de web, con unos 10 millones de usuarios reportados.

- ***NIST:*** El Instituto Nacional de Normas y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology), llamada entre 1901 y 1988 Oficina Nacional de Normas (NBS por sus siglas del inglés National Bureau of Standards), es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.
  Como parte de esta misión, los científicos e ingenieros del NIST continuamente refinan la ciencia de la medición (metrología) creando una ingeniería precisa y una manufacturación requerida para la mayoría de los avances tecnológicos actuales.

- ***Open-source:*** Código abierto es la expresión con la que se conoce al software distribuido y desarrollado libremente. Se focaliza más en los beneficios prácticos (acceso al código fuente) que en cuestiones éticas o de libertad que tanto se destacan en el software libre.

- ***Perl:*** es un lenguaje de programación diseñado por Larry Wall en 1987. Perl toma características del lenguaje C, del lenguaje interpretado bourne shell (sh), AWK, sed, Lisp y, en un grado inferior, de muchos otros lenguajes de programación.

- ***RSA:*** (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

- ***SHA:*** El SHA (Secure Hash Algorithm, Algoritmo de Hash Seguro) es una familia de funciones hash de cifrado publicadas por el Instituto Nacional de Estándares y Tecnología (NIST). La primera versión del algoritmo fue creada en 1993 con el nombre de SHA, aunque en la actualidad se la conoce como SHA-0 para evitar confusiones con las versiones posteriores. La segunda versión del sistema, publicada con el nombre de SHA-1, fue publicada dos años más tarde. Posteriormente se han publicado SHA-2 en 2001 (formada por diversas funciones: SHA-224, SHA-256, SHA-384, y SHA-512) y la más reciente, SHA-3, que fue seleccionada en una competición de funciones hash celebrada por el NIST en 2012. Esta última versión se caracteriza por ser la que más difiere de sus predecesoras.

- ***SQL:*** El lenguaje de consulta estructurado o SQL (por sus siglas en inglés Structured Query Language) es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ellas.

- ***UIT-T:*** es el órgano permanente de la Unión Internacional de Telecomunicaciones (UIT) que estudia los aspectos técnicos, de explotación y tarifarios, y publica normativas sobre los mismos, con vista a la normalización de las telecomunicaciones a nivel mundial.

- ***X509:*** es un estándar UIT-T para infraestructuras de claves públicas (en inglés, Public Key Infrastructure o PKI). X.509 específica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación.

ANEXOS

ANEXO I: DETALLES DE INSTALACIÓN Y CONFIGURACIÓN DE EJBCA

Primero se detalla la instalación del Sistema Operativo, en este caso el elegido fue GNU/Linux en su distribución CentOS usando la versión 6.5.

Según lo que se detalló en el punto 4.1 del Anexo II, se realiza una instalación mínima del Sistema Operativo, configurando apropiadamente la red y el firewall. Luego, se procede a instalar EJBCA en sí:

a) Software necesario para la instalación de la AC:
   - **Kit de desarrollo OpenJDK versión Java 1.6**
   - **Servidor de aplicaciones Jboss** versión **7.1.1 Final**
   - **Ant versión** **ant-1.9.3-2.fc21.noarch.rpm**.
   - **Motor de Base de Datos MySQL versión 5.1.73-3.el6_5**
   - **Java MySQL Connector** driver JDBC de **mysql-connector-java.noarch**

b) La instalación se realizó siguiendo los pasos de la guía de instalación "Installing EJBCA 6.1.1 and Jboss on CentOS 6.5", ubicada en el sitio web http://ejbcacentos.blogspot.com.ar **[18]**.

c) Una vez instalado EJBCA siguiendo los pasos anteriores tenemos dado de alta la Autoridad de certificación ManagementCA que se utiliza para emitir certificados para la autenticación de los operadores de EJBCA.

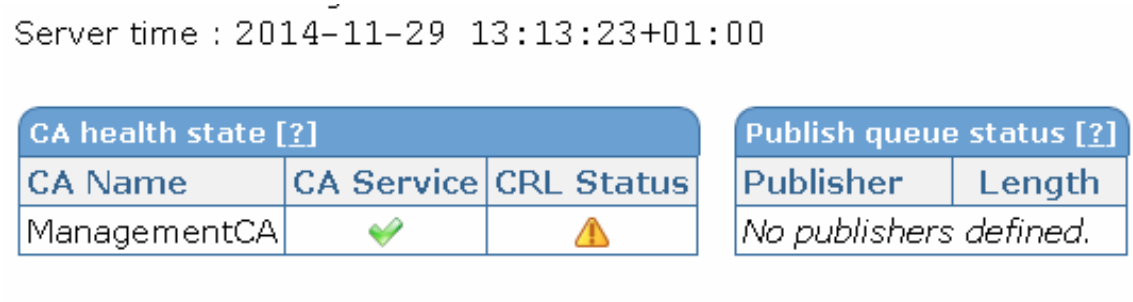

Figura N° 13 – Creación de la AC "ManagementCA"

d) Se ingresa con el certificado emitido en la instalación de superadmin y se procede a crear el perfil de la Autoridad de Certificación del IUA. Se tuvieron en cuenta las recomendaciones de la guía de instalación de Branko Majic, "Setting-up EJBCA as Certification Authority" [19] y el trabajo de Juan Osorio, "Evaluación de la herramienta EJBCA para un Prestador de Servicios de Certificación" [20], para la configuración de perfiles y especificaciones de certificados en EJBCA.

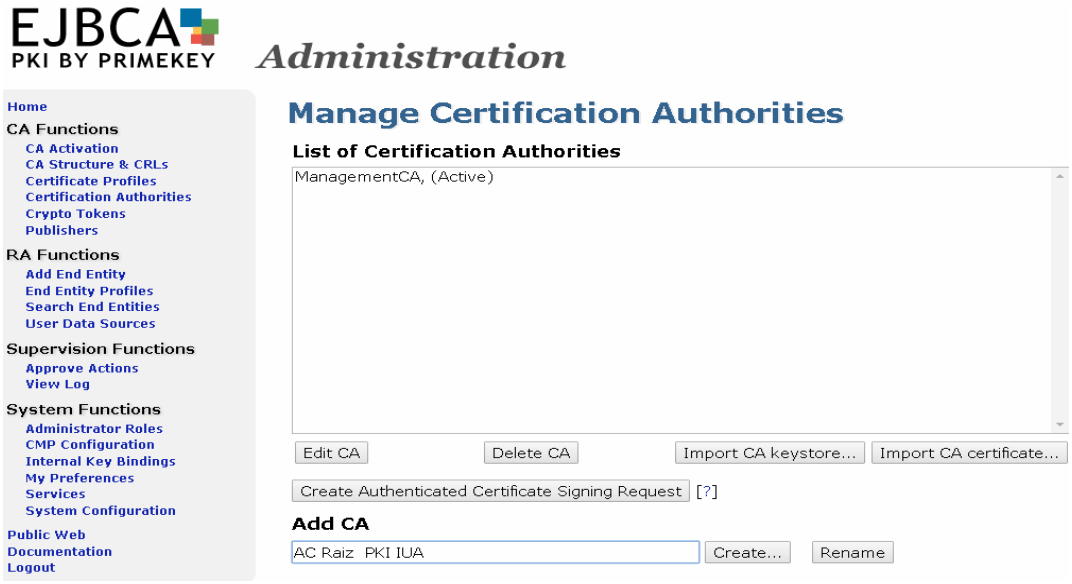

Figura N° 14 – Creación del perfil de Autoridad de Certificación del IUA

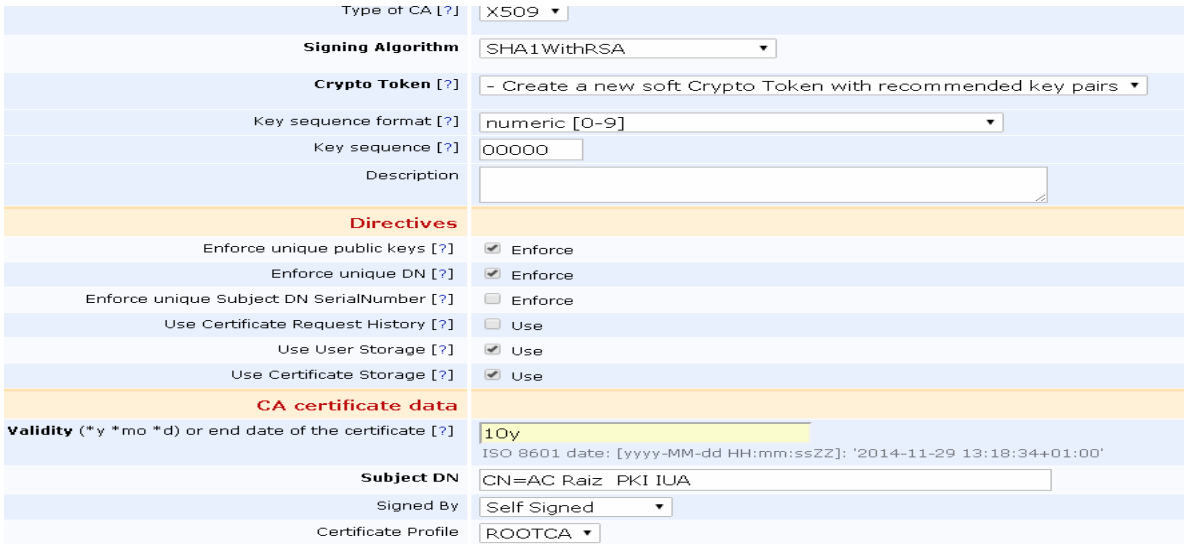

Figura N° 15 - Creación del perfil de Autoridad de Certificación del IUA (cont.)

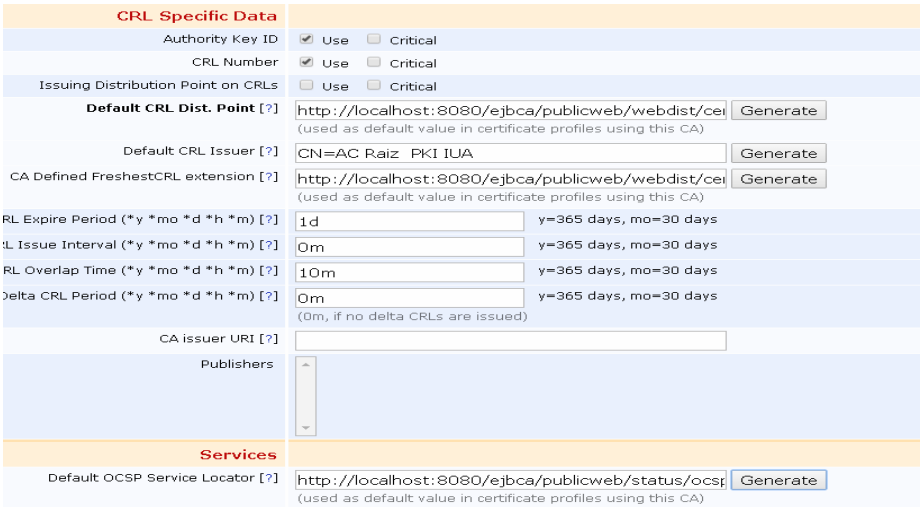

Figura N° 16 - Creación del perfil de Autoridad de Certificación del IUA, detalles de CRL

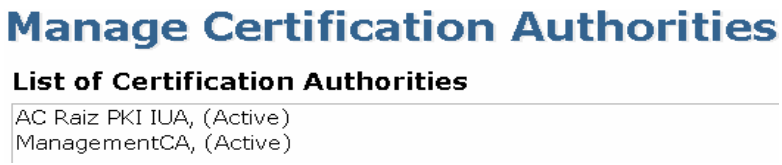

Figura N° 17 - Listado de Autoridades de Certificación generadas en EJBCA

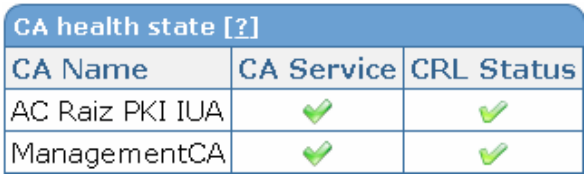

Figura N° 18 - Estado de Autoridades de Certificación en EJBCA

e) Se crea el perfil de certificado de Docente.

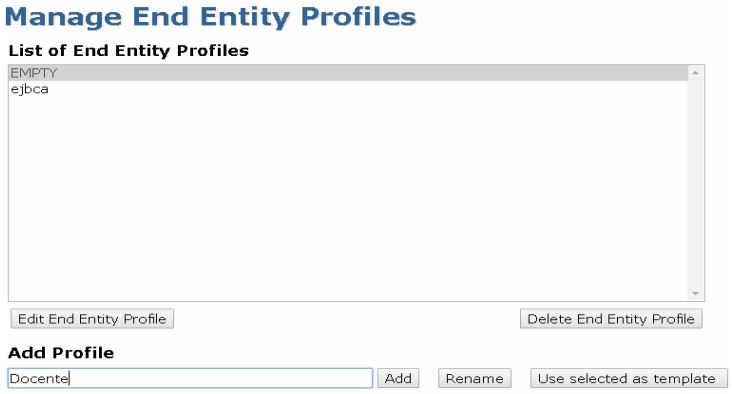

Figura N° 19 – Creación del perfil de docente y empleado en EJBCA

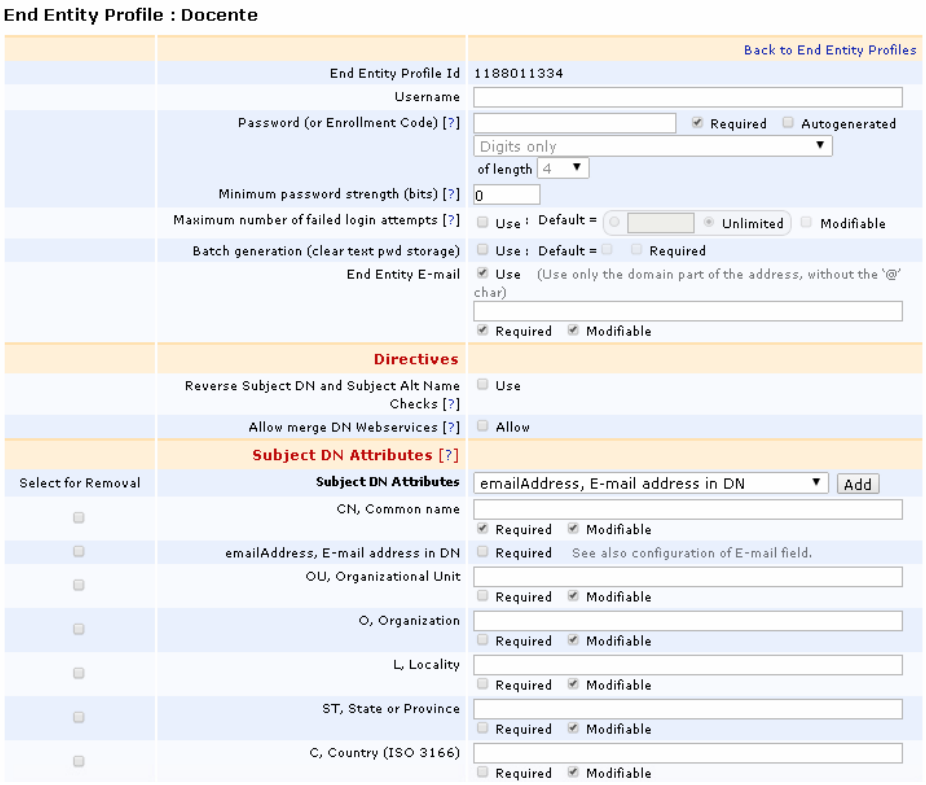

Figura N° 20 – Configuración de perfil de docente

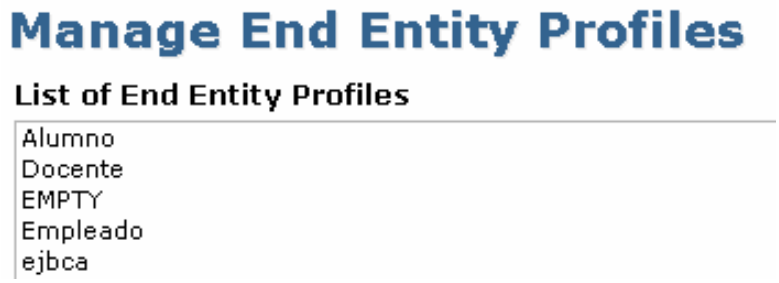

Figura N° 21 – Listado actualizado de perfiles creados en EJBCA

ANEXO II: CONFIGURACIÓN DE VIRTUAL MACHINES

Para el armado de la red virtual se utilizó la aplicación VMWare ESXi 5.5.0, quedando el ambiente de red del presente proyecto virtualizado.

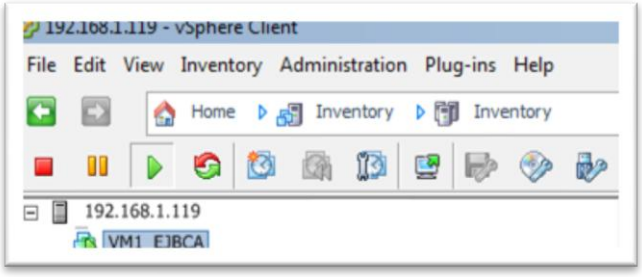

Figura N° 22 – Virtual machine utilizada para el laboratorio

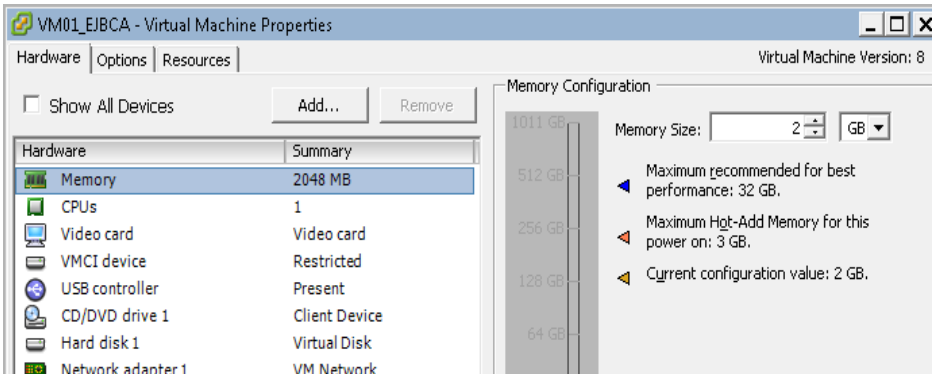

Figura N° 23 – Configuración de la VM01 (EJBCA)