Universidad Central "Marta Abreu" de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

TRABAJO DE DIPLOMA

Niveles de Implementación de una Infraestructura de Llave Pública para la Intranet de la UCLV

Autor: Elizabet de Armas Sardiñas.

Tutor: Msc Ramón Torres Rojas.

Santa Clara

2009

"Año del 50 Aniversario de la Revolución"

Universidad Central "Marta Abreu" de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

TRABAJO DE DIPLOMA

Niveles de Implementación de una Infraestructura de Llave Pública para la Intranet de la UCLV.

Autor: Elizabet de Armas Sardiñas.

edearmas@uclv.edu.cu

Tutor: Msc Ramón Torres Rojas.

rtorres@uclv.edu.cu

Consultante: Ing Erisbel Orozco Crespo.

Santa Clara

2009

"Año del 50 Aniversario de la Revolución"

Hago constar que el presente trabajo de diploma fue realizado en la Universidad Central "Marta Abreu" de Las Villas como parte de la culminación de estudios de la especialidad de Ingeniería en Telecomunicaciones y Electrónica, autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

_____

Firma del Autor

Los abajo firmantes certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

_____ _____

Firma del Tutor

Firma del Jefe de Departamento donde se defiende el trabajo

_____

Firma del Responsable de Información Científico-Técnica

PENSAMIENTO

"La posibilidad de realizar un sueño es lo que hace que la vida sea interesante."

Paulo Coelho

DEDICATORIA

A mis abuelos Eliza y Fermín por haber sido siempre mi fuente de inspiración y mi apoyo.

Y a mi papá, por su dedicación y cariño ..

AGRADECIMIENTOS

- ***A mi mamá por su incondicionalidad***
- ***A mi hermana por quererme como soy***
- ***A mi tío por toda la ayuda que me ha brindado***
- ***A mi familia por su apoyo***
- ***A mis profesores por su acertada guía***
- ***A mis amigos por todos los momentos compartidos***
- ***A mi tutor por brindarme la oportunidad***

A todos

Gracias

TAREA TÉCNICA

Se realizó una detallada revisión bibliográfica sobre el tema de la PKI para la construcción del marco teórico referencial. Luego de haber estudiado las posibles variantes, se procedió a desarrollar los diferentes niveles de implementación práctica y se evaluó cada nivel integrado a cada uno de los servicios que fueron probados. Todas las pruebas fueron evaluadas de acuerdo a su calidad, requerimientos computacionales, compatibilidad, entre otros aspectos, en el ensayo a escala de laboratorio. Finalmente se procedió a la elaboración de la propuesta para la Intranet de la UCLV.

Firma del Autor

Firma del Tutor

RESUMEN

El presente trabajo trata sobre los niveles de implementación de una Infraestructura de Llave Pública (PKI) integrada a la Intranet de la UCLV. En síntesis se realizo una presentación de los principales conceptos y principios de la PKI. Se procedió al análisis de las diferentes metodologías y soluciones en materia de implementación, vinculadas con los principales servicios de la Intranet. Se determinó las políticas de seguridad que deben quedar operativas con la implementación de la infraestructura. Por ultimo se describen las pruebas realizadas y los resultados en cada caso, concluyéndose con la propuesta definitiva.

.

TABLA DE CONTENIDOS

INTRODUCCIÓN

El crecimiento alcanzado por la red del Ministerio de Educación Superior en estos últimos años es notable. La Intranet de la Universidad Central "Marta Abreu" de las Villas, como parte de esta red, se ha integrado junto con sus usuarios a este desarrollo, adoptando las nuevas tecnologías que han ido surgiendo. A su vez las necesidades en materia de seguridad son cada vez más exigentes; por lo que el uso de un mecanismo de seguridad más completo, como es una Infraestructura de Llave Pública (PKI) que sirva como soporte habilitador para útiles aplicaciones sobre la propia red, que no están actualmente desarrolladas, constituiría un importante paso de avance .

En la UCLV siempre se ha trabajado con vistas de incrementar la seguridad de la Intranet. En la actualidad se han realizado varios estudios sobre propuestas de implementación de la PKI como infraestructura de seguridad. En los mismos se tuvo en cuenta que la infraestructura brindara autentificación, integridad, confidencialidad y otro elementos muy ventajosos; que pueden ser habilitados aplicando el principio de las llaves públicas a la mayoría de los servicios, recursos y a los usuarios de la red. Todo ello sin entorpecer al usuario final ni a los sistemas. Sin embargo, ¿cuáles son las variantes de implementación más adecuadas para lograr una mayor integración con los principales servicios que ofrece la red?

Lo anteriormente expuesto da paso a otras interrogantes:

- ¿Cuál es la situación actual en el desarrollo de los niveles de implementación de las PKI?
- ¿Qué soluciones reales en materia de seguridad de la Intranet fundamenta el uso de este tipo de infraestructura?
- ¿Cuál sería la propuesta definitiva de implementación de la infraestructura y su integración con los principales servicios en la intranet de la UCLV?

Por ello el objetivo general de este trabajo es implementar una PKI que sirva de base de seguridad para los principales servicios que se brindan en la Intranet. Esto implicó un estudio teórico sobre el tema en cuanto a los conceptos y consideraciones para la implementación. Se hicieron pruebas con algunas de las posibles soluciones a escala de

laboratorio que ayudasen a comprender mejor estos sistemas. La solución está determinada de acuerdo a las necesidades y características de la Intranet.

El trabajo está estructurado en: introducción, capitulario, conclusiones, recomendaciones, referencias bibliográficas, glosario de términos y anexos. A continuación se muestra un resumen breve del contenido de cada uno de los capítulos.

CAPÍTULO I:

Se presentará brevemente los principales conceptos y principios de la PKI. Se hará un análisis sobre el estado del arte en general. En esta parte se demostrará la relativa madurez y estabilidad alcanzada en el tema.

CAPÍTULO II:

Se hará una discusión y comparación más profundas sobre las diferentes metodologías y soluciones en materia de implementación. Se determinan las políticas de seguridad que deben quedar operativas con la implementación de la infraestructura.

CAPÍTULO III:

Se describirán las pruebas a realizar así como los resultados en cada caso concluyendo con la propuesta definitiva.

CAPÍTULO 1 INTRODUCCIÓN A LA INFRAESTRUCTURA DE LLAVE PÚBLICA (PKI).

1.1 Seguridad informática

La seguridad informática constituye, en nuestros días, un obligatorio tema de estudio para la correcta puesta en marcha de cualquier sistema informático. Estos sistemas están sujetos constantemente a la posibilidad de experimentar un funcionamiento anómalo, ya sea de manera fortuita o provocada. El principal objetivo de la seguridad informática consistirá en evitar que se produzcan tales situaciones (López, 2008).

Los sistemas informáticos incorporan medidas para garantizar su seguridad prácticamente a todos los niveles, desde el hardware hasta los interfaces de usuario, pasando por todas las capas del Sistema Operativo y los elementos dedicados a las comunicaciones, por solo mencionar algunos. (Goots et al., 2003)

1.1.1 Ataques y amenazas

En un sistema que maneja información ciertos procesos no deben ocurrir. Resultaría inaceptable, por ejemplo, que los datos que se introducen en el mismo sufrieran alteraciones cuando se van a recuperar, o que fuera posible para terceros consultar la información (López, 2008).

Dentro de las categorías generales de ataques más conocidas podemos mencionar la interrupción, intercepción, modificación y suplantación, que en su carácter de pasivos o activos, cada uno se identifica por el nivel de intromisión realizada por agentes externos.

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener la información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico. Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información. Por otra parte los ataques activos, implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos (Cruz, 2005).

Estas amenazas y ataques, pueden ser realizados en sistemas aislados, o en sistemas interconectados (redes), que es donde los sistemas presentan más vulnerabilidades. Así mismo dependiendo del entorno, se podrían dar ataques externos o físicos relacionados con la protección de los soportes físicos de la información, más que a la información propiamente.

1.2 Macanismos y herramientas de seguridad

Tres propiedades fundamentales deben proporcionar a la información los sistemas informáticos: confidencialidad, integridad y disponibilidad; por ello los mecanismos para garantizar su seguridad no pueden ser ajenos a estos sistemas, pues estos pueden frenar y minimizar de alguna manera, las amenazas y ataques a la información (López, 2008).

Algunos de los mecanismos y herramientas mas utilizados para proteger estos sistemas son los siguientes:

- Definición de niveles de seguridad.
- Claves de acceso (*password*s).
- Criptografía y firma digital en las comunicaciones
- Utilización de Certificados para la autenticación.

El nivel de desarrollo de estos mecanismos depende del plan de seguridad trazado teniendo en cuenta la naturaleza de la organización, el tipo de información , los usuarios que usan y acceden a esta, las aplicaciones, asi como los equipos y sistemas con que se cuenta. La puesta en marcha de un plan de seguridad no es algo estático que se hace una vez, sino que va evolucionando en dependencia de las exigencias organizativas (Rojas, 2004).

Un plan de seguridad debe de especificar las tareas a realizar, sus responsables, cómo se definen los niveles de acceso, cómo se realizará el seguimiento, dónde deben ponerse en marcha medidas específicas (cortafuegos, *firewalls*, filtros, control de acceso y otros), e inclusive tomar en cuenta la estructura organizativa.

La viabilidad es un punto que no podemos olvidar, se pueden llegar a proponer medidas muy seguras pero realmente impracticables (Cruz, 2005).

1.3 Criptografía como base matemática para la seguridad

La criptografía abarca el estudio de técnicas matemáticas relacionadas a aspectos de la seguridad, tales como confidencialidad, integridad de datos, autenticación, y no repudio.

Los algoritmos criptográficos combinan matemáticamente datos de texto simple de entrada y una clave secreta para generar datos codificados (texto cifrado). Con un buen algoritmo criptográfico, no es posible computacionalmente invertir el proceso de encriptación y derivar los datos de texto simple, empezando únicamente con el texto cifrado; algunos datos adicionales y una clave, son necesarios para llevar a cabo la transformación

1.3.1 Criptografía simétrica.

La criptografía simétrica se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que llamaremos clave o llave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para codificar como para decodificar (Nash et al., 2001).

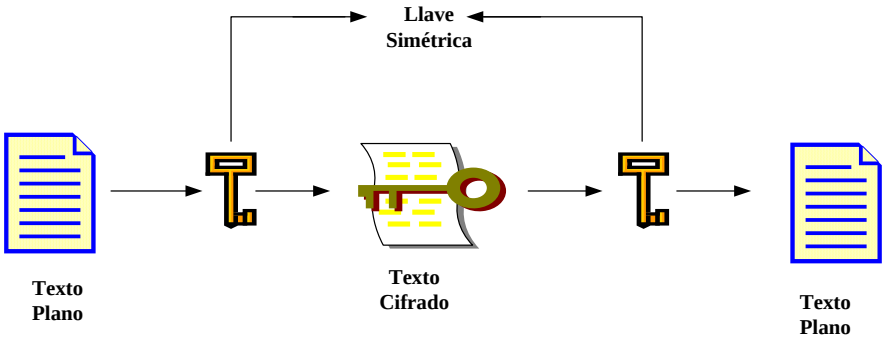

Figura 1.1 Criptografía simétrica

Aunque las claves simétricas puedan poseer algunas características muy deseables (como un pequeño tamaño de realización y velocidades de codificación/decodificación que pueden alcanzar decenas de megabytes por segundo o más), ellas también sufren de algunos inconvenientes significativos en algunos ambientes tales como:

- La necesidad de cambio de clave secreta:

Antes de iniciar la transmisión de un mensaje tanto el remitente del mismo, como el destinatario deben conocer la llave simétrica por lo que el transporte de esta llave requiere de una comunicación separada y segura que debe ocurrir antes de que se establezca la comunicación intencionada. Este paso adicional aunque factible en algunos ambientes, puede ser muy difícil o muy inoportuno en algunas circunstancias.

- Dificultades en iniciación de comunicación segura entre partes desconocidas:

La necesidad de un intercambio de clave secreta separado, puede conducir a grandes dificultades cuando las partes son desconocidas, es decir cuando las entidades no han tenido ningún contacto anterior.

- Dificultades de escala:

Ejemplifiquemos este problema de la siguiente manera: la llave secreta compartida entre un usuario A y un usuario B difiere de la utilizada por el mismo usuario A con otro usuario C. En una comunidad de 1,000 usuarios, entonces, el usuario A tendría que mantener potencialmente 999 llaves secretas (realmente, 1000 si desea codificar datos sólo para él), por lo que podemos concluir que en una comunidad de *n* usuarios se pueden llegar a tener como mínimo $n*(n-1)$ llaves secretas. Cuando la comunidad crece, el almacenaje y el mantenimiento de un número tan grande de llaves pueden hacerse rápidamente complejo. Los problemas de manejabilidad se hacen aún más pronunciados porque las llaves no duran para siempre, periódicamente son sustituidas por otras para limitar la cantidad de datos codificados con una misma llave. (Adams and Lloyd, 2002).

1.3.2 Criptografía asimétrica

Su principal característica es que a diferencia de la criptografía simétrica las claves no son únicas, sino que forman pares, denominadas clave privada y clave pública. Una de ellas se emplea para codificar, mientras que la otra se usa para decodificar. Dependiendo de la aplicación que se le de al algoritmo, la clave pública será la de cifrado o viceversa (Figura 1.2)

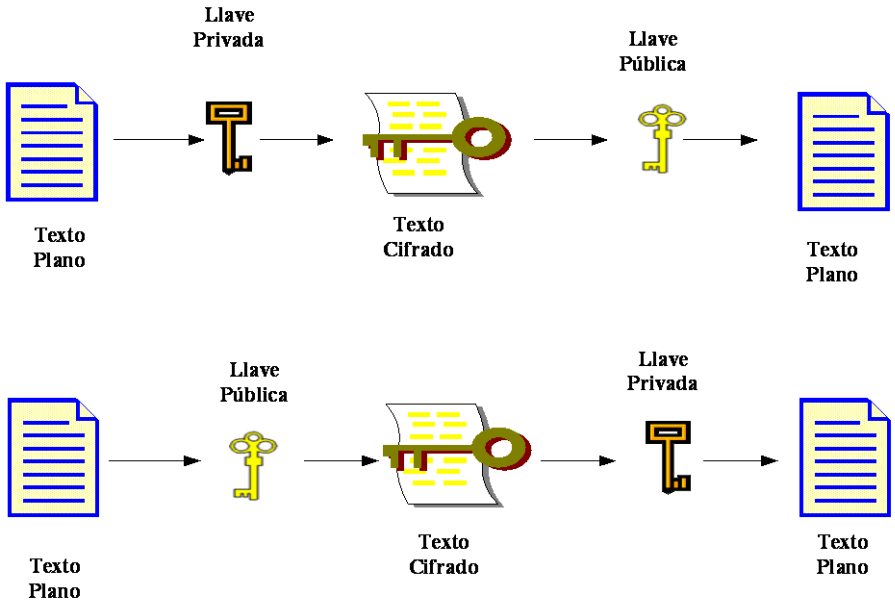

Figura 1.2 Criptografía asimétrica.

Este par de claves son lo suficientemente diferentes que conocer una no permite la derivación o el cálculo de la otra. Incluso para adversarios decididos, con mucho poder de cómputo a su disposición, esta acción es casi imposible. Esto significa que una de las llaves puede darse a conocer y estar disponible (por ejemplo, almacenada en una base de datos pública) sin reducir la seguridad del par, siempre y cuando la otra llave permanezca privada. (Nash et al., 2001)).

Con la criptografía asimétrica fue posible para cualquier sistema tomar la llave pública de cualquier usuario y diseminarla extensamente. De esta forma si dos entidades no han tenido ninguna comunicación anterior, una puede buscar la llave pública de la otra y proteger datos para ella.

Hay por supuesto una advertencia, se debe estar seguro de que la llave pública que se obtiene realmente pertenece al usuario con el cual se quiere establecer comunicación. Hay dos mecanismos generales para conseguir esto:

- Confiar en la información que devuelve el depósito público.

- Encontrar un modo de verificar que la información obtenida es correcta. Se puede no confiar en el depósito público, pero la información que este devuelve se verifica de forma independiente.

En entornos convencionales, un depósito público confiable es alcanzable, al menos en algún grado. En el mundo electrónico, sin embargo, tal modificación de datos no autorizada es una preocupación legítima No se puede confiar en que los depósitos públicos, en general, siempre devuelvan la información correcta; por ello, la información que el mismo brinda debe ser independientemente verificable. Algunos mecanismos utilizados para la autentificación son la firma digital y las funciones resumen. (Nash et al., 2001)).

1.3.3 Funciones resumen

Como se ha mencionado una de las aplicaciones de la criptografía asimétrica es la autentificación de mensajes, con ayuda de funciones resumen (*hash*, en inglés), que basan su funcionamiento en el principio de la compresión. Estas funciones dan como resultado bloques de longitud fija *a* a partir de bloques de longitud fija *b*, con $a < b$ (2005). El mensaje resultante es mucho más pequeño que el mensaje original, y es muy difícil encontrar otro mensaje diferente que dé lugar al mismo resumen. Algunas funciones *hash* conocidas son: MD4, MD5, SHA-1, SHA-224, 256, 384, 512, *Whirlpool*, etc. (Mironov, 2005)

Supongamos que un usuario A recibe un mensaje *m* de un usuario B y quiere comprobar su autenticidad. Para ello B genera un resumen del mensaje al que llamaremos *r (m)* y lo codifica empleando la clave de codificación, (llave privada). La clave de decodificación que se ha hecho pública previamente, debe estar en poder de A. El usuario B envía entonces al usuario A, el resumen correspondiente *r (m).* A puede ahora generar su propio resumen *r0 (m)* y compararlo con el valor *r (m)* obtenido del resumen que le fue enviado con anterioridad; si coinciden, el mensaje será auténtico.

1.3.4 Firma digital

La separación entre claves públicas y privadas en la criptografía ha permitido la creación de nuevas aplicaciones. La creación y validación de firmas digitales constituye una de ellas.

La firma digital se basa en una transformación matemática que combina la clave privada con los datos que se van a firmar en tal forma que:

- Sólo la persona que posee la clave privada pudo haber creado la firma digital.
- Cualquiera con acceso a la clave pública correspondiente puede verificar la

firma digital (2007).

- Cualquier modificación de los datos firmados (incluso cambiar únicamente un

solo *bit*) invalida la firma digital.

Las firmas digitales son en sí únicamente datos, por lo que pueden transportarse junto con los datos firmados a los que protegen. Por ejemplo, un usuario A puede crear un mensaje de correo electrónico firmado para un usuario B y enviar la firma junto con el texto del mensaje, proporcionando al destinatario la información que se requiere para verificar el origen del mismo.

Las firmas digitales permiten verificar que los datos no fueron alterados (ya sea accidental o intencionalmente) mientras se encontraban en el tránsito desde el origen hacia destino, por lo tanto, pueden utilizarse para proporcionar un mecanismo muy seguro de integridad de datos (Bertolín and Bertolín, 2004)).

La mayoría de las aplicaciones que realizan firmas digitales usan una combinación de algoritmos simétricos y funciones resumen. El algoritmo *hash* provee un mecanismo para determinar si el mensaje original ha sido alterado de cualquier manera, mientras que el cifrado asimétrico protege el resumen resultante de ser modificado y prueba que fue creado por el remitente de la información. En otras palabras, la firma digital brinda la posibilidad de verificar la autenticidad del origen e integridad de la información. La figura 1.3 muestra la interacción entre funciones *hash* y el cifrado asimétrico en el proceso de firma digital. (Komar and Team, 2004).

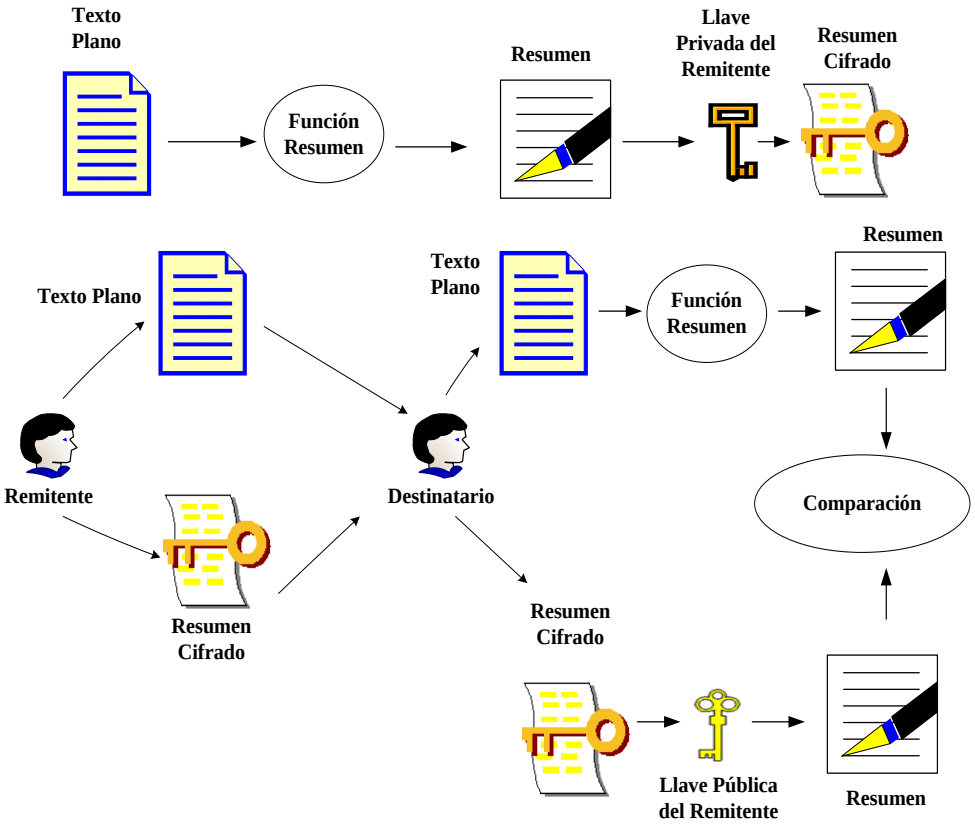

Figura 1.3 Proceso de firma digital

1.3.5 Otros servicios

El descubrimiento de la criptografía de clave pública puso a disposición algunos servicios que eran desconocidos o inalcanzables con criptografía simétrica.

La criptografía asimétrica puede ser usada para realizar el establecimiento de una comunicación privada entre dos entidades; es decir el protocolo puede usar llaves públicas y privadas tal que, en la conclusión del mismo, las dos entidades comparten una llave simétrica secreta conocida por ninguna otra entidad.

Otros servicios interesantes incluyen la construcción de los generadores de número pseudos arbitrarios, protocolos para juegos, mecanismos para conducir elecciones electrónicas seguras, y técnicas que permiten a una entidad demostrar a otra entidad que conoce un

secreto sin necesidad de revelar dicho secreto (conocido como conocimiento cero o protocolos de conocimiento mínimo) (Adams and Lloyd, 2002).

1.4 Infraestructura de seguridad

Un sustrato dominante constituye el soporte base para cualquier empresa; una infraestructura puede ser vista como tal. La definición de una infraestructura de seguridad es bastante amplia. Abarca aspectos tales como: nombramiento consecuente, políticas de seguridad, monitoreo, auditoria, administración de los recursos, revisión, control de acceso de dispositivos, etc.

Las ventajas que fluyen de un acercamiento infraestructural a la seguridad son variadas y numerosas. La infraestructura proporciona un apuntalamiento de seguridad para toda la organización, hace la seguridad disponible en el acto a aplicaciones individuales, refuerza y simplifica el proceso de autentificación, proporciona la transparencia de usuario final, y ofrece seguridad completa a todos los objetos del ambiente (Adams and Lloyd, 2002).

1.5 Infraestructura de llave pública

En los últimos años, las infraestructuras de clave pública (PKI) han cobrado una gran importancia. De un modo sencillo, se puede describir a una infraestructura de clave pública (*Public Key Infrastructure*) como el conjunto de componentes y políticas necesarias para crear, gestionar y revocar certificados digitales que pueden ser utilizados para autenticar cualquier aplicación, persona, proceso u organización de una red de empresa, extranet o internet (Lioy et al., 2006)). Como bien lo dice su nombre las PKI basan su funcionamiento en los principios y técnicas de llaves públicas.

Una PKI totalmente funcional, abarca un número grande de componentes y servicios con los cuales debe lidiar:

- Autoridades de Certificación
- Depósitos de Certificados
- Autoridades de Registro
- Revocación de Certificados
- Reserva y Recuperación de Claves

- Actualización Automática de Clave
- Apoyo al No Repudio
- Marcador de Tiempo Seguro
- Software de Cliente

Puede ser correctamente argumentado que algunos ambientes específicos no necesitan toda esta funcionalidad. Por ejemplo, un PKI que brinde correo electrónico seguro entre amigos probablemente tiene poca necesidad del apoyo al no repudio. Sin embargo, una verdadera PKI conceptualmente diseñada como entidad infraestructural independiente debe ser capaz de desplegarse en cualquier ambiente. Así, tiene sentido implementar una PKI con el mayor número de componentes posibles. En cualquier despliegue dado, cualquier servicio innecesario entonces puede ser fácilmente apagado o no instalado en absoluto (Adams and Lloyd, 2002).

La figura 1.4 muestra un esquema básico de una PKI.

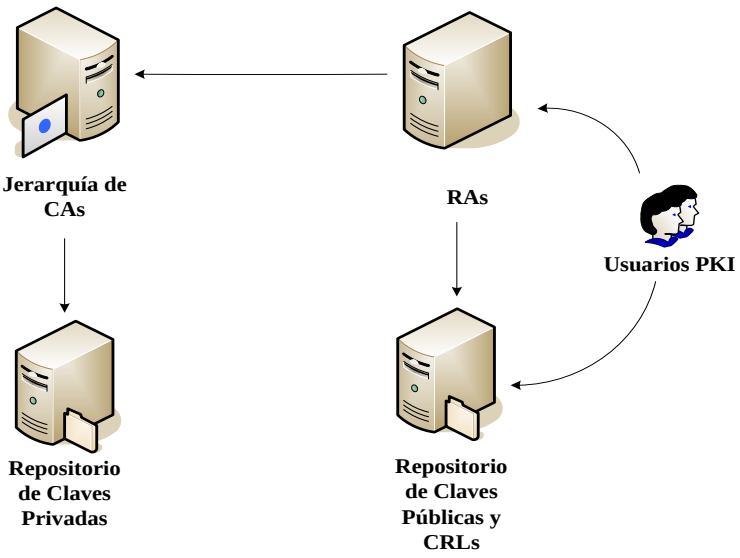

Figura 1.4 Esquema Básico PKI.

1.6 Principales componentes y servicios.

1.6.1 Autoridades de certificación

Un certificado constituye un medio de transporte para una clave pública, similar a un sobre que contiene una carta con la clave pública escrita. Un certificado contiene además del par de llaves, un conjunto de atributos que identifican al propietario y establecen el uso para el que se destina al certificado. Estos atributos son confiables pues el certificado está firmado digitalmente por la entidad emisora con su clave pública. Existen varios tipos de certificados de acuerdo al formato: Certificados X.509, certificados *Simple Public Key Infrastructure* (SPKI) y certificados *Pretty Good Privacy* (PGP) (Lucas, 2006).

La premisa fundamental en la formulación original de la criptografía asimétrica era que dos entidades desconocidas deberían ser capaces de comunicarse sin problemas. Cuando una entidad desea establecer comunicación con otras mediante la criptografía de clave pública, debe obtener primero un certificado digital. Con una población potencial de usuarios de cientos o miles de entidades es designando un pequeño número de autoridades para realizar la generación de certificados. Se les denomina a dichas autoridades, Autoridades de Certificación (CA). La CA es responsable de administrar todos los aspectos del ciclo de vida del certificado después de su expedición.(Slagell et al., 2006)

1.6.2 Depósitos de certificados

La CA soluciona sólo la parte del problema mencionado en la sección anterior, es decir a menos que una entidad pueda localizar con facilidad el certificado correspondiente a la clave pública de otra, es como si ese certificado nunca hubiera sido creado. Alguna clase de sistema de depósito robusto (base de datos), escalable y en línea debe estar disponible para la localización eficaz de los certificados. Varias tecnologías pueden ser utilizados con el fin de crear estos depósitos: X.500, LDAP (*Lightweight Directory Access Protocol)*, servidores *web*, servidores de FTP, DNS, y otros (Zeilenga, 2006).

1.6.3 Autoridad de registro

Aunque el proceso de registro pueda ser desempeñado directamente por la CA, normalmente tiene sentido delegar la función de registro a un componente separado referido como Autoridad de Registro (RA). Esta entidad es la encargada de verificar los datos de los usuarios que solicitan el certificado para posteriormente aprobarlos y exportarlos a la CA para que sea firmado y emitido al usuario correspondiente (Lodos et al., 2003).Como en el caso de las CA es muy común tener en una misma PKI, múltiples Ras, por ejemplo, cuando el número de entidades finales de una PKI crece considerablemente y/o están dispersas geográficamente, la noción del registro centralizado se hace problemática. El despliegue juicioso de múltiples RAs ayuda a solucionar el problema. (Adams and Lloyd, 2002).

1.6.4 Revocación de certificados

Los certificados emitidos por la CA no deben durar eternamente para mayor seguridad, por lo que se editan con una fecha de expiración (Espinoza et al., 2008). No obstante en algunas ocasiones deben ser revocados inmediatamente .Las razones de una revocación de certificados son las siguientes:

- **Llave Privada Comprometida**: la llave privada puede ser robada, o es por otro medio (perdida de *smart card*) adquirida por una persona no autorizada.
- **Autoridad Certificadora Comprometida**: la llave privada de la CA se ve comprometida. Esto puede ocurrir cuando se brindan servicios de certificados o por la perdida de dispositivos de almacenamiento, como discos duros, *smart card* (Rankl and Effing, 2003), etc. Si el certificado de la CA se compromete todos los certificados publicados por esta son revocados por no ser considerados confiables. (Abadi et al.)
- **Cambio de Afiliación**: el objeto al cual se le emitió un certificado (normalmente un usuario) realizó un cambio de organización.
- **Reemplazo**: ocurre cuando se realiza un cambio en la extensión de certificados por lo que se debe reemplazar el certificado existente, o cuando se realiza un cambio en el nombre del usuario asociado al certificado.

- **Cese de Operación**: los certificados salen de operación cuando el servidor *web* es sustituido por uno nuevo u ocurre una fusión y el nombre del DNS anterior es deshabilitado requiriendo un reemplazo para todos los certificados de la *web*.
- **Asimiento (*hold*) de Certificados**: esta revocación es temporal y ocurre cuando se determina que un certificado no va a ser utilizado por un periodo de tiempo determinado.

Debe haber un modo de alertar al resto de los usuarios que ya no aceptable utilizar una llave pública para comunicarse con una entidad determinada. Este mecanismo que alerta en un PKI es llamado Revocación de Certificados (Housley et al., 2002).Para tratar tales situaciones, la autoridad mantiene actualizada una lista de revocación de certificados (*Certificate Revocation List – CRL*), que los usuarios pueden consultar para asegurarse de que un determinado certificado sigue siendo válido en ese momento. Las CRL son accesibles por diferentes medios de consulta, como correo electrónico, *web* o LDAP (Hagström, 2006)).

Es importante señalar que existen 2 tipos de CRL:

- **CRL base**: contiene los números de serie de todos los certificados revocados en la CA, así como la razón de cada revocación y la llave privada vinculada con la misma .Esta lista especifica en cada caso todos los certificados firmados por esa llave. Si el certificado es renovado y se le asigna un nuevo par de llaves, un nuevo CRL es generado que incluye solo información concerniente a los certificados revocados que hayan sido firmados con el nuevo par de llaves.
- **CRL delta:** Contiene solo el número de serie y los motivos de revocación de los certificados revocados desde que el último CRL base fue publicado. Este tipo de CRL proporciona la información de revocación mas actualizada y disminuye la cantidad de información a descargar.

1.6.5 Reserva y recuperación de claves

En cualquier ambiente PKI operacional dado, puede esperarse que un porcentaje de usuarios, cada período de tiempo fijo (por ejemplo, cada mes o cada año), se encuentren imposibilitados de utilizar su llave privada. Este puede ser debido a numerosas situaciones:

- Las contraseñas olvidadas de la llave privada criptografiada de un usuario dado, están todavía físicamente almacenadas, pero son inaccesibles.
- La destrucción de un disco duro o de una tarjeta inteligente (Al-Khouri and Bal, 2007).
- Una computadora es remplazada por otra mas moderna y los certificados no son trasferidos antes que el viejo disco duro sea formateado

En un ambiente determinado se pueden codificar documentos de gran importancia bajo la llave pública de un usuario particular. Si la llave privada correspondiente es perdida, aquellos documentos no son recuperables lo que constituye una pérdida significativa. (Adams and Lloyd, 2002).

Una solución a este problema es codificar todos los datos para recipientes múltiples, pero este no siempre puede ser práctico (por ejemplo, para datos muy confidenciales).Una solución mucho mas práctica y comúnmente utilizada es habilitar la reserva y la recuperación de llaves privadas.

1.6.6 Actualización automática de clave

Un certificado tiene un tiempo de vida finito. Este puede ser por motivos teóricos, o bien, puede ser por motivos basados en valoraciones prácticas, como la limitación de la cantidad de datos típicamente protegidos por una sola llave. Independientemente de la razón, en muchos ambientes PKI, un certificado dado tendrá que "expirar" y ser sustituido por un nuevo certificado. Este procedimiento es llamado una actualización de clave o una actualización de certificado.

La mayor parte de los usuarios PKI encuentran incómodo y molesto el procedimiento de actualización manual de cada uno de sus certificados. Los usuarios normalmente no recuerdan la fecha en la cual su certificado expira, y muchos lo averiguan cuando es demasiado tarde (es decir cuando el certificado deja de validar). Por lo tanto, hasta que no completen el procedimiento de actualización, estarán fuera del servicio en lo que a la PKI se refiere. Además, cuando un usuario está en este estado, el procedimiento de actualización es ligeramente más complicado, requiriendo un cambio de CA, similar al proceso de inicialización. (Nash et al., 2001).

La solución es poner en práctica la PKI de tal modo que la actualización de certificado o llave es manejada de un modo totalmente automatizado por la PKI misma, sin la intervención del usuario. Siempre que el certificado del usuario esté a punto de ser usado para cualquier objetivo, su período de validez es comprobado. Cuando la fecha de caducidad se acerca, una operación de renovación ocurre, y un nuevo certificado es generado. Entonces, el nuevo certificado es usado en el lugar del viejo, y la transacción solicitada por usuario continua. La actualización Automática de Clave es vital en una PKI operacional en muchos ambientes. (Adams and Lloyd, 2002).

1.6.7 Apoyo al no repudio

Los usuarios de un PKI con frecuencia niegan acciones que irrevocablemente están vinculadas a su identidad. Esta acción recibe el nombre de repudio. Por ejemplo, un usuario A firma digitalmente un documento, asegurando así que el documento provino de él. Para el flujo liso e ininterrumpido de la PKI, existe una exigencia que no permite a los usuarios romper arbitrariamente esta asociación en el futuro. Meses después de firmar el documento, el usuario no debe ser capaz de negar que la firma realmente provino de él.

Una PKI debe proporcionar el apoyo al no repudio. La infraestructura no puede proporcionar por sí misma el no repudio verdadero; típicamente, un elemento humano es necesario para emitir un juicio a partir de pruebas. Es deber de la PKI apoyar este proceso proporcionando algunas pruebas técnicas requeridas, como la autenticación de origen de datos y una atestiguación confiable del tiempo en el que los datos fueron firmados.

1.6.8 Marcador de tiempo seguro

Un elemento crítico en el apoyo a servicios de no repudio es el uso de un marcador de tiempo seguro dentro de la PKI. Es decir los usuarios deben confiar en la fuente de tiempo, y el valor de tiempo debe ser bien comunicado. Debe existir una fuente autoritaria de tiempo en la que una población de usuarios PKI confiará. La fuente autoritaria de tiempo para el PKI (es decir el servidor seguro que marca el tiempo cuyo certificado es verificable por la comunidad relevante de usuarios PKI) no tiene que existir únicamente para los objetivos del no repudio; muchas situaciones surgen, en los cuales una etiqueta de tiempo autoritario en un documento puede ser útil. (Nash et al., 2001)

Irónicamente, el tiempo suministrado por la fuente autoritaria dentro de la PKI no tiene que ser correcto; simplemente tiene que ser aceptado por la población de usuarios como el tiempo de referencia para sus acciones dentro de la PKI.

1.6.9 *Software* de cliente

Una PKI puede ser visto, al menos en algún nivel, como una colección de servidores que brindaran un servicio para un usuario, sin embargo, como toda arquitectura de servidor-cliente, los servidores no pueden hacer nada para el cliente a menos que el cliente reclame el servicio (es decir, que realice una petición). El cliente en la plataforma local del usuario debe solicitar servicios de certificación, tratar la información de revocación relevante, exigir una actualización automática de clave o una operación de recuperación clave y conocer cuando se requiere una marca de tiempo en un documento. (Adams and Lloyd, 2002).

El software de cliente es un componente esencial de PKI, el cual existe fuera de cada aplicación y pone en práctica al cliente final requiriendo de los servicios PKI. Las aplicaciones se unen a este software de cliente por puntos de entrada estandarizados, pero estos clientes usan la infraestructura; no son parte de la misma

Es importante notar que la necesidad del software de lado de cliente no implica nada sobre el tamaño o alcance del mismo. Hay muchas posibilidades de como el software del lado del cliente es puesto en práctica e invocado, pero debe estar disponible como un componente independiente fuera de todas las aplicaciones de PKI.

1.7 Aplicaciones y tecnologías

Una Infraestructura de Llave Pública permite el despliegue de aplicaciones y el uso de tecnologías tales como:

- EFS (*Encrypting File System*): codifica datos utilizando métodos de inscripción simétricos y asimétricos. El EFS proporciona dos métodos de recuperación usando una autoridad certificadora en *Windows 2003*: recuperación de datos, en la cual un agente de recuperación de datos designado puede abrir todos los archivos criptografiados en la esfera; y la recuperación clave, en donde un agente de

recuperación clave puede recuperar el archivo de la llave privada de la base de datos de CA.

- Autenticación y codificación *web*: Mediante SSL (*Secure Socket Layer*) se envía información encriptada, así como se autentica uno o ambos extremos de un canal de comunicación. SSL es la base para HTTPS, FTPS, SMTPS, POPS, etc.
- S/MIME (*Secure/Multipurpose Internet Mail Extensiones*): Proporciona la comunicación confidencial, la integridad de datos, y no rechazo para mensajes de correo electrónico. Permite realzar la seguridad del correo electrónico usando certificados para verificar las cartas credenciales del remitente, el punto del mensaje de origen, y autenticidad de mensaje (Xenitellis, 2001).
- SET *(Secure Electronic Transaction*), protocolo para compra y pago con tarjetas de crédito a través de Internet. Favorece el comercio electrónico.
- IPSec: extensiones de seguridad para el protocolo IP, implementa confidencialidad a nivel de red, permite crear túneles seguros a través de redes inseguras para comunicar redes remotas. (Ettl, 2003)
- WTLS (*Wireless Transport Layer Security*): componente opcional de la pila de protocolos WAP, similar a SSL con consideraciones especiales para dispositivos inalámbricos. (Goffee et al., 2004b)
- 802.1x autenticación mediante puerto: permite a usuarios y computadoras debidamente certificadas el acceso a redes inalámbricas o a redes Ethernet. Esto proporciona la identificación de usuario centralizada y la autenticación usando RADIUS (*Remote Authentication Dial-In User Service*).

1.8 Políticas de seguridad y PKI

Una infraestructura llave pública (PKI) es tan segura como las políticas y procedimientos que son puestos en práctica en su implementación Tres documentos de cumplimiento obligatorio definen las políticas de seguridad en una PKI:

1. **Política de Seguridad:** Una organización típicamente tiene varios documentos de política de seguridad, los cuales proporcionan definiciones completas de cuestiones de seguridad, los riesgos y amenazas afrontadas por la organización, y las medidas que deben ser tomadas para proteger datos y recursos de la misma.

2. **Política de Certificación (CP)***:* este documento describe las medidas que una organización usará para validar la autenticidad de un certificado así como los permisos que este posea para desarrollar determinadas aplicaciones.
3. **Declaración de Prácticas con Certificados (CPS):** este documento describe como una Autoridad de Certificación dentro de una organización sostiene las políticas de seguridad y de certificación.

Dos de los recursos el más comúnmente usados para definir una política de seguridad son la ISO 27002 "Co*de of Practice for Information Security Management*" y la RFC 2196 "*The Site Security Handbook*". La ISO 27002 proporciona información detallada y recomendaciones para desarrollar políticas de seguridad; por otra parte la RFC 2196 aunque más orientada hacia la PC, describe varios tipos de recursos que deberían ser cubiertos en una política de seguridad total, así como recomendaciones para asegurar dichos recursos. Las políticas de seguridad, las políticas de certificado, y CPSs son típicamente creados por miembros de la organización teniendo en cuenta los recursos legales, humanos, y tecnológicos con que cuenta la entidad. (Komar and Team, 2008).

CAPÍTULO 2 JERARQUÍAS DE AUTORIDADES CERTIFICADORAS

2.1 Niveles jerárquicos de la CA

En una Infraestructura de Llave Pública, el diseño e implementación de una jerarquía de Autoridades Certificadoras (CA) constituye una consideración de primer orden. Cuestiones tales como el número de niveles de la jerarquía, la cantidad de CA individuales presentes en cada nivel, el tipo de certificado que publicará cada CA y las políticas de seguridad que se utilizaran para la protección de la misma, requiere un cuidadoso despliegue de recursos.

La mayor parte de las jerarquías tienen de dos a cuatro niveles, sin embargo, jerarquías de CA de un nivel son recomendables para organizaciones pequeñas que manejan menos de 300 cuentas de usuarios y que solo requieren servicios PKI básicos. En este tipo de jerarquía solo se instala una CA como raíz de la organización (*Enterprise Root CA*) que permanece dentro del dominio y que desde el punto de vista administrativo no presenta grandes exigencias. Esta CA se encarga de la publicación, renovación y revocación de certificados, así como de la publicación de las CRLs. En cuanto a seguridad, las organizaciones tan pequeñas normalmente no necesitan la implementación de una CA de políticas (Cross and Kinder, 2004)

La jerarquía de un nivel aunque es muy fácil de administrar presenta el inconveniente de que si la CA presenta fallos, los servicios de certificados no estarán disponibles para tratar peticiones de certificados entrantes hasta que la CA sea restablecida al servicio.

Las jerarquías de CA de dos niveles constan de una CA raíz, autónoma y sin conexión, y de una o varias CA emisoras en línea. Estas CA emisoras establecen una cadena de confianza con la CA raíz y realizan la labor de autoridades de políticas y emisoras de certificados.

Para aumentar la disponibilidad de los servicios de certificados dos o más autoridades emisoras deben ser instaladas, de esta forma si una falla, las otras estarán disponibles. El numero de CA emisoras depende de las exigencias de la organización.

Las jerarquías de CA de tres niveles están compuestas por una CA raíz, autónoma y sin conexión, por una o varias CA de políticas intermedias, autónomas y sin conexión y por una ó varias CA emisoras en línea que permanecen dentro del dominio. Las ventajas que este tipo de jerarquía proporciona son varias:

- Seguridad física a la infraestructura pues sus dos primeros niveles (raíz y políticas) se encuentran sin conexión protegiéndolos así de los ataques en línea.
- Requiere que se hayan definido dos o más políticas de seguridad para emitir un certificado.
- Permite la definición de políticas de CA, de políticas de certificados y la de varias declaraciones de prácticas de certificados (CPSs).
- La gestión de la jerarquía de CAs es dividida entre equipos diferentes de administradores de red. En este escenario cada uno de estos equipos es responsable de definir las CPS para sus CAs de políticas de certificados.

La figura 2.1 muestra una jerarquía de autoridades certificadoras de tres niveles.

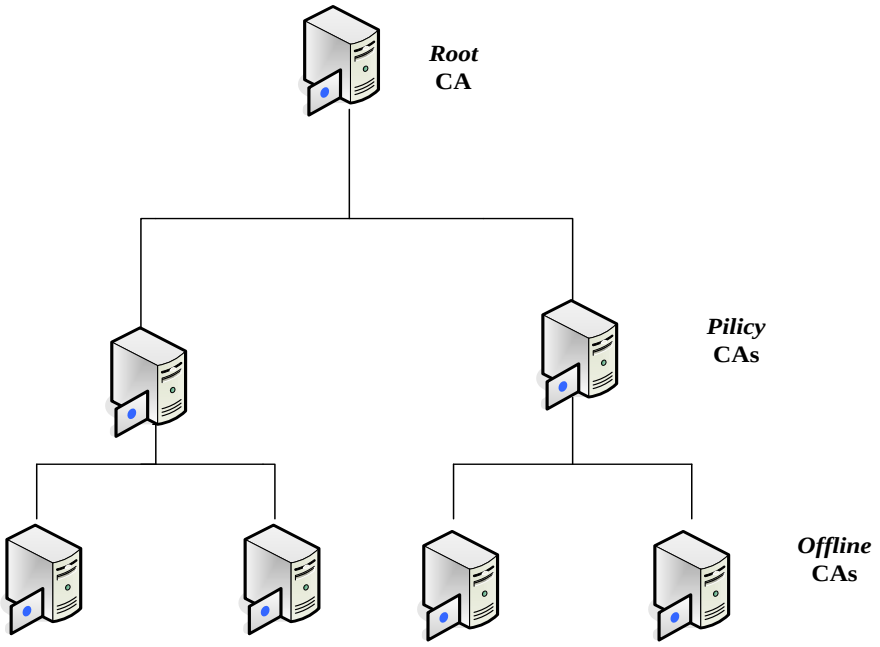

Figura 2.1 Jerarquía de CAs

Una jerarquía de CA de cuatro niveles puedes ser necesaria en algunos casos, pero el despliegue de jerarquías mayores no es recomendable.

2.2 Implementación de una jerarquía de Cas en *Windows Server 2003*

El número de niveles en la jerarquía de autoridades certificadoras depende de la cantidad de certificados a emitir, la estructura de la organización y el número de categorías diferentes de usuarios y servicios a tratar (Hellen, 2004).

Para la instalación de jerarquías de uno, dos y tres niveles de CAs se recomienda el siguiente orden de operaciones (Komar and Team, 2004):

- **Jerarquía de un nivel de CA:**

1. Preparación de los *scripts* de Configuración de la CA (*CA Configuration Files)*.
2. Implementación de la CA raíz (*Enterprise Root* CA).
3. Verificación de la instalación.

- **Jerarquía de dos niveles de CAs:**

1. Preparación de los *scripts* de Configuración de la CA (*CA Configuration Files)*.
2. Implementación de la CA raíz (*Standalone Root* CA).
3. Implementación de las CAs emisoras (*Issuing* CA).
4. Verificación de la instalación.

- **Jerarquía de tres niveles de CAs:**

1. Preparación de los *scripts* de Configuración de la CA (*CA Configuration Files)*.
2. Implementación de la CA raíz (*Standalone Root* CA).
3. Implementación de las CAs de políticas (*Policy CA*).
4. Implementación de las CAs emisoras (*Issuing* CA).
5. Verificación de la instalación.

2.3 Jerarquía de un nivel de CA.

2.3.1 Preparación de los *script* de configuración de la CA

La preparación de los archivos de configuración de la CA es aplicable a todos los diseños de jerarquías de CA, sin importar el número de niveles que tenga. En esta primera etapa de la implementación, se procede a la configuración de la autoridad certificadora mediante archivos de texto (*scripts*), los cuales garantizan que los ajustes deseados queden

especificados en la configuración de cada CA, y que, en caso de un fracaso dicha configuración sea recuperable.

CAPolicy.inf es el archivo que proporciona la información de configuración de los servicios de certificado, el cual es leído durante la instalación inicial de la CA y siempre que se renueve un certificado de la misma. Algunas de las informaciones que en él se especifican son:

- Lugar de publicación de la Lista de Revocación de Certificados (CRL).
- Intervalo de publicación de los CRL.
- Lugar de publicación de los certificados de la CA raíz (AIA y CDP).
- Los limites para el uso de los certificados.
- Los ajustes de renovación de certificado como período de validez y tamaño clave.
- Información sobre la declaración de Prácticas con Certificados (CPS).

Cuando se instala un Servidor de *Windows* 2003, el archivo *CAPolicy.inf* no existe, por lo que se debe crear manualmente. Este archivo de texto debe ser guardado en el directorio % *windir* % del sistema operativo (C:\Windows\capolicy.inf).Otros puntos a tener en cuenta es que la máquina contenga al menos dos particiones, no pertenezca a ningún dominio (excepto que sea una CA raíz de una jerarquía de un nivel), el nombre de la misma y el grupo de trabajo deben ser revisados previamente pues no pueden ser cambiados después de la instalación; la fecha y la hora deben ser las correctas y la instalación debe ser realizada por un miembro del grupo de administradores locales. En el Anexo I se muestra el contenido de *CAPolicy.inf* para cada autoridad en la jerarquía.

2.3.2 Servicios de Información de Internet (IIS)

El proceso de implementación de una PKI con su jerarquía de CAs correspondiente solo necesita para el despliegue de certificados configurar correctamente los servicios de certificados de *Windows Server 2003*, sin embargo si se desea desplegar la Inscripción *Web* de servicios de certificados, para poder realizar el despliegue de los mismos mediante la *web*, es necesario realizar una instalación mínima de los Servicios de Información de Internet (IIS).

Para realizar esta instalación se accede a menú inicio *Control Panel\ Add or Remove Programs\ Add/Remove Windows Components\ Application Server\ Details*. En la ventana de *Application Server* se despliegan las especificaciones de *Internet Information Services,* en las cuales se debe garantizar que estén seleccionadas las siguientes opciones:

- *Common Files.*
- *Internet Information Services Manager.*
- *World Wide Web Service.*

El siguiente paso lo constituye *World Wide Web Service\ Details* donde, para dar por terminada la instalación, se activan las opciones de:

- *Active Server Pages.*
- *World Wide Web Service.*

Para que funcione correctamente este servicio debe ser instalado antes de comenzar la implementación de la jerarquía de autoridades certificadoras.

2.3.3 Implementación de la CA raíz (*Enterprise Root CA*)

Aunque el despliegue que se desea realizar sea de un nivel es recomendable crear el archivo *CAPolicy.inf* con el objetivo de guardar los cambios de configuración correspondiente a la CA raíz. En este caso, el *CAPolicy.inf* especifica que el tamaño de la llave es de 2048 *bits*, el periodo de validez del certificado es de 10 años, las CRLs base son publicadas cada 2 días y las CRLS deltas cada 12 horas. La CA raíz no tendrá extensiones AIA (*Authority Information Access*) o CDP (*CRL Distribution Point*) y no son necesarias las CPSs.

Luego de que el archivo *CAPolicy.inf* haya sido creado y salvado correctamente se procede a la instalación de los servicios de certificados. El proceso comienza en el menú inicio de *Windows Server* 2003\ *Control Panel\Add or Remove Programs\Add/Remove Windows Components\Certificate Services.* El tipo de CA es *Enterprise Root CA* y queda habilitada la opción *Use Custom Settings To Generate the Key Pair.* En *Public and Private Key Pair* se seleccionan las siguientes opciones*:*

- CSP: *Microsoft Strong Cryptographic Service Provider.*
- *Allow the CSP to interact with the desktop:* Deshabilitada.

- *Hash algorithm: SHA-1.*
- *Key length:* 2048.

La información de identificación de la CA está compuesta por el nombre común, el sufijo DN y el período de validez .Un ejemplo de configuración aplicable a la Intranet de la UCLV es *UCLV Root CA, DC=UCLV, DC=EDU, DC=CU* y 10 *Years* respectivamente. La configuración de la base de datos de la CA es la que aparece por defecto.

Una vez instalados los servicios de certificados se procede a ejecutar el *script* de pos instalación mostrado en el Anexo II. Este proceso permite que los ajustes de configuración sean definidos correctamente en la CA raíz y que queden activos todos los procesos de revisión para los servicios de certificados en dependencia del acceso exitoso o no a los objetos del sistema.

Como la autoridad raíz pertenece al dominio, las auditorias deben ser realizadas en un objeto del Grupo de Políticas (GPO) unido a la Unidad Organizacional (OU) que contiene en su Directorio Activo la cuenta, de la computadora donde radica la CA.

El procedimiento para definir un GPO en el dominio donde radica la CA se inicia en *Administrative Tools \ Active Directory Users and Computers \ OU \ Properties.* En la ventana de propiedades de la unidad organizacional se abre un nuevo grupo de políticas (*Group Policy\ New*) con el nombre de *CA Audit Settings.* Luego se procede a editar el nuevo GPO a través de *Computer Settings\Windows Settings\Security Settings\Local Policies\Audit Policy* permitiendo los siguientes ajustes para la realización de auditorias, basados en la guía de Seguridad del *Windows Server 2003:*

- *Account Logon: Success, Failure*
- *Account Management: Success, Failure*
- *Directory Service Access: Failure*
- *Logon Events: Success, Failure*
- *Object Access: Success, Failure*
- *Policy Change: Success, Failure*
- *Privilege Use: Failure*
- *Process Tracking: No auditing*
- *System Events: Success, Failure*

2.4 Jerarquías de CAs de tres niveles.

Por un problema practico-metodológico, en la estructura de este capítulo se ha decidido analizar la implementación de la jerarquía de tres niveles antes que la de dos niveles. Las razones para establecer este orden en el análisis del tema son las siguientes:

- Los *scripts* de Configuración (*CAPolicy.inf*) y el proceso de implementación la CA raíz (*Standalone Root* CA) son los similares en ambas jerarquías.
- Una vez que se hayan implementado las CAs de políticas y las CAs emisoras en una jerarquía de tres niveles, es mas fácil comprender y realizar la implementación de las CAs emisoras de la jerarquía de dos niveles, las cuales a la vez desempeñan el papel de autoridades de políticas.

Es importante recordar que las computadoras donde se instalan las autoridades certificadoras raíz, en ambos niveles, no deben estar conectadas a la red ni pertenecer a dominio alguno.

2.4.1 Implementación de la CA raíz (*Standalone Root CA*)

Para la CA raíz el *CAPolicy.inf* especifica que la llave privada tiene un tamaño de 4,096 bits, su certificado tiene un periodo de validez de 20 años, la CRL base se publica cada 6 semanas, las CRLs delta están deshabilitadas y el certificado no contiene extensiones CDP y AIA asegurándose de esta forma que el certificado de la CA raíz le es confiado al usuario que esta instalando esta autoridad, para su protección.

Este proceso de instalación de los servicios de certificados es similar al anterior, con la variante de que en este caso el tipo de CA es *Standalone Root CA* y que el tamaño de la llave en *Public and Private Key Pair* es de 4096 bits. En *CA Identifying Information* el nombre de la CA será *UCLV Root CA*, *DC=UCLV*, *DC=EDU*, *DC=CU* y el periodo de validez de 20 años. La base de datos de certificados, los archivos de eventos o *logs* y los archivos de configuración serán establecidos en D: \CertDB, D:\CertLog y D:\CAConfig respectivamente.

Luego de la instalación se ejecuta el *script* de postinstalación del Anexo II para que queden habilitadas las auditorias de eventos de los servicios de certificados.

La configuración de las políticas de seguridad local para auditar el acceso, exitoso o no, a objetos del sistema se lleva a cabo de la misma forma que en *Enterprise Root CA*.

2.4.2 Implementación de la Cas de políticas (*Policy CA*)

Luego de instalar la autoridad raíz, se procede a la instalación de las autoridades de políticas sin conexión (*Policy* CA), para lo cual, es necesario establecer confianza en el certificado de la CA raíz y en la base de datos de la misma. Esta operación se realiza manualmente, copiando el certificado en un disco *floppy* para su traslado e instalándose en la máquina local. Otra acción necesaria es publicar la CRL de la CA raíz para asegurar que los chequeos de revocación son realizados correctamente.

El siguiente *script* permite la publicación del certificado de la CA raíz y de su CRL en la base de datos ubicada en la máquina donde radicará la CA de políticas:

```
@echo off
a:
cd \
for %%c in (*.crt) do certutil -addstore -f Root “%%c"
for %%c in (*.crl) do certutil -addstore -f Root “%%c”
```

El *CAPolicy.inf* correspondiente a este nivel de la jerarquía define un CPS mediante un OID (Identificador de objetos) y un URL donde el CPS es almacenado. Solo es implementado un OID por cada CA de políticas, la longitud de su llave privada es de 2048 bits, el periodo de validez de su certificado es de 10 años, las CRLs base se publican cada 6 semanas y la CRLs delta están deshabilitadas.

La diferencia en cuanto a las instalaciones de servicios de certificados anteriores radica en que el tipo se CA es *Standalone Subordinate CA* y el tamaño de la llave es de 2048 bits. En la información de la CA se especifica que el nombre de la misma es *UCLV Policy1 CA* y el periodo de validez *Determine by Parent*. En la ventana *Certificate Database Settings* se especifican nuevamente las localizaciones D: \CertDB, D:\CertLog y D:\CAConfig. En *CA Certificate Request* se salva el certificado en un disco *floppy* (A:\policyca.req) para su

traslado a autoridad raíz la cual, de esta forma, reconoce a la autoridad de política como su subordinada y genera un certificado que debe ser instalado en la CA de políticas.

Para realizar esta operación se accede mediante el menú inicio a *Administrative Tools* *Certification Authority*\ *UCLV Root CA* (menú contextual) *All Tasks*\ *Submit New Request.* En el *Open Request File* se selecciona A:\PolicyCA.req \ *Open*. En la nueva ventana se despliega *UCLV Root CA* y se accede a *Pending Requests*\ *Certificate Request*\ *All Tasks*\ *Export Binary Data*\ *Columns That Contain Binary Data*\ *Binary Request*. Esta opción permite verificar que hayan sido correctamente configuradas las propiedades de la CAs de políticas y se garantiza que sus políticas de seguridad (CP y CPS) funcionan correctamente. Realizado este análisis se retorna a *Pending Requests**SubCA certifícate*\ *All Tasks*\ *Issue**Issued Certificate*\ *Details* (pestaña)\ *Copy to File*\ *Certificate Export Wizard*\ *Export File Format*\ *Cryptographic Message Syntax Standard-PKCS #7 Certificates* (Johner et al., 2001), para incluir en la base de datos, todos los certificados encontrados a lo largo de la cadena de confianza. En la ventana *File to Export* el tipo de archivo que se selecciona es A:\policyca.p7b para salvar el certificado en disco *floppy*.

Una vez que se tiene el certificado se procede a instalarlo en la autoridad de políticas para que esta comience a brindar servicio. El camino es similar al anterior: *Administrative Tools*\ *Certification Authority*\ *UCLV Policy CA* (menú contextual)\ *All Tasks* \ *Install CA Certificate.* En la ventana *Select File to Complete CA Installation* el archivo que se selecciona es A:\policyca.p7b; luego sobre *UCLV Policy CA*, se selecciona *All Tasks y* queda activado el servicio.

En el proceso de posinstalación la autoridad de políticas asume que en la red de la universidad:

- Todos los servidores y computadoras personales soportan *Windows 2000*, *Windows XP* o *Windows Server 2003* y pertenecen al dominio uclv.edu.cu.
- Dentro del dominio UCLV existe un servidor *web* con el nombre *certpub.uclv.edu.cu* que contiene dentro de él, un directorio virtual con el nombre de *CertDATA* que constituye el CDP y AIA de todas las CAs de la jerarquía. Este servidor es de fácil acceso.
- Las CAs subordinadas a las CAs de políticas tienen un periodo de validez de 5 años.

- El certificado de la autoridad de política y su CRL son copiados en un, *floopy* para su traslado y posterior publicación en el Directorio Activo y en *certpub.uclv.edu.cu.*
- *Windows Server 2003 Resource Kit* está instalado.

Para el proceso de posinstalación se ejecuta el *script* mostrado en el Anexo II. Luego solo resta configurar las políticas de seguridad local para auditar el acceso, exitoso o no, a objetos del sistema.

2.4.3 Implementación de las Cas emisoras (*Issuing CA*)\

Antes de instalar los servicios de certificados de la CA emisora, esta debe confiar en la autoridad raíz y ser capaz de descargar el certificado de la autoridad de políticas así como su CRL para poder realizar chequeos de revocación. El proceso de establecer confianza se realiza manualmente publicando los certificados y las CRLs de las CA raíz y de políticas en una base de datos local, en el Directorio Activo o en los URLs especificados en las extensiones AIA y CDP.(Karatsiolis et al., 2004)

El siguiente *script* permite la instalación local de los certificados y CRLs de las autoridades raíz y de políticas:

```
@echo off
a:
cd \
for %%c in (“ROOTSRV*.crt”) do certutil -addstore -f Root “%%c"
for %%c in (“UCLV Root*.crl”) do certutil -addstore -f Root “%%c"
for %%c in (“POLICY*.crt”) do certutil -addstore -f CA “%%c"
for %%c in (“UCLV Policy*.crl”) do certutil -addstore -f CA “%%c”
```

El método más utilizado para la publicación de estos documentos es mediante el Directorio Activo en el cual la publicación se realiza a través de la configuración del contexto de nombre, que permite descarga automática a todos los objetos del dominio que soporten *Windows* 2000, XP ó *Server* 2003. El siguiente *script* de instalación debe ser ejecutado por un miembro del grupo de administradores de dominio:

```
@echo off
```

```
a:
cd \
for %%c in (“ROOTSRV*.crt”) do certutil -dspublish -f “%%c” RootCA
for %%c in (“UCLV Root*.crt”) do certutil -dspublish -f “%%c” SubCA
for %%c in (“POLICY*.crl”) do certutil -dspublish -f “%%c"
for %%c in (“UCLV Policy*.crl”) do certutil -dspublish -f “%%c"
gpupdate /force
```

Si la publicación de la información se realiza mediante los URLs especificados en las extensiones AIA y CDP, los métodos no pueden ser especificados pues factores referentes al servidor *web* tales como, su localización en la infraestructura de red, el dominio, el grupo de trabajo al que pertenece y el sistema operativo que soporta, deben ser tomados en cuenta.

El *CAPolicy.inf* correspondiente a las CAs emisoras especifican que la longitud de su llave privada es de 2048 *bits*, su certificado tiene un periodo de validez de 5 años, las CRLs base se publican cada 3 días y las CRLs deltas cada 12 horas. El archivo correspondiente se muestra en el Anexo I.

Si se desea realizar el despliegue de certificados a través de la *web* es necesario instalar en la autoridad emisora, IIS para poder acceder a las páginas de inscripción de servicios de certificados (ver epígrafe 2.3.2)

En los servicios de certificados se especifica que el tipo de CA es *Enterprise Subordinate CA*, el nombre de la misma es *UCLV Issuing CA* y se activa el *Active Server*.

En esta ocasión le corresponde a la autoridad de políticas realizar la petición del certificado y a la vez emitir un nuevo certificado que debe ser publicado en la autoridad emisora, quedando de esta forma finalizado el proceso de reconocimiento de la misma por los niveles superiores.

El proceso de pos instalación se lleva a cabo ejecutando el *script* mostrado en el Anexo II. En este proceso se asume que en la red UCLV:

- Todos los servidores y computadoras personales soportan *Windows 2000*, *Windows XP* ó *Windows Server 2003* y pertenecen al dominio uclv.edu.cu.

- El certificado de la autoridad emisora y su CRL están publicados en el Directorio Activo, en la *web* perteneciente a la CA emisora y en otro servidor *web* que sea accesible externamente.
- Dentro del dominio UCLV existe un servidor *web* con el nombre *certpub.uclv.edu.cu* que contiene dentro de él, un directorio virtual con el nombre de *CertDATA* que constituye el CDP y AIA de todas las CAs de la jerarquía. Este servidor es de fácil acceso.
- La CA emisora publica certificados a usuarios, computadoras, servicios y dispositivos de red con un periodo de validez máximo de dos años.
- *Windows Server 2003 Resource Kit* está instalado.
- La recuperación de los certificados y las CRLs se realizaran en el siguiente orden:
    1. Directorio Activo.
    2. Servidor *web* accesible.
    3. El servicio *web* perteneciente a la autoridad emisora.
    4. La carpeta UNC (*Universal Naming Convention*) presente en la autoridad emisora.

Como la autoridad emisora esta dentro del dominio, la configuración de las políticas de seguridad local para auditar el acceso a objetos del sistema, deben ser realizadas en un objeto del Grupo de Políticas unido a la Unidad Organizacional que contiene en su Directorio Activo, la cuenta de la computadora donde radica la CA.

2.4.4 Verificación de la instalación

Una vez culminada la instalación de la jerarquía de CAs de tres niveles se procede al la verificación de la instalación. Se debe comprobar que los URLs especificados en las extensiones AIA y CDP fueron correctamente configurados, y si es posible, siguiendo la cadena de confianza, acceder correctamente a los certificados y CRLs correspondientes.

Una herramienta muy útil es *PKI Health Tool* incluido en *Windows Server 2003 Resource Kit* .Su instalación debe ser hecha desde una computadora que pertenezca al dominio.

Para utilizar *PKI Health Tool* se debe inicializar el vínculo (*link*) dinámico asociado a la librería DDL mediante el siguiente procedimiento: en la ventana de comandos ejecutar

regsvr32 pkiview.dll, el cual permite la instalación y registro de forma automática de *PKI Health Tool* y la librería DDL correspondiente. Luego para utilizar la herramienta se ejecuta el comando *pkiview.msc.*

Esta herramienta de verificación permite comprobar el estado de cada AIA y CDP-URL. Los estados posibles son los siguientes:

- *OK*: el certificado de la CA ó el CRL correspondiente a un URL determinado, son válidos.
- *Expiring*: el certificado de la CA ó el CRL correspondiente al URL determinado, están cerca de la fecha de expiración.
- *Unable to download*: el certificado de la CA ó el CRL correspondiente al URL determinado, no pueden ser descargados.

2.5 Jerarquía de dos niveles de Cas

Cuando se despliega una jerarquía CA de dos niveles, la implementación de la CA raíz (*Standalone Root CA*) se realiza de la misma forma que en la jerarquías de tres niveles. El segundo nivel de la misma es desplegado como una combinación de autoridades de política y emisoras de certificados, por lo que el cambio de configuración principal lo constituye le contenido del *CApolicy.inf* (ver Anexo II*).* En el se especifica que la longitud de la llave es de 2048 *bits*, el periodo de validez de la misma es de 5 años, las CRLs base se publican cada 3 días y las CRLs delta se publican cada 12 horas. En este nivel de la jerarquía se define un OID correspondiente a un CPS y el URL donde es almacenado este OID.

Los procesos de verificación de la instalación (auditorias) se realizan de manera similar a las analizadas anteriormente.

2.6 Plantillas de Certificados

Las plantillas de certificados son usadas por las Infraestructuras de Llave Publica montadas sobre *Windows Server 2003* para definir el contenido de los certificados publicados por las autoridades certificadoras. *Microsoft Management Console* (MMC) constituye una herramienta muy útil para definir y personalizar servicios de certificados (Kinder and Cross, 2004)

El servidor de *Windows 2003* define dos tipos de plantillas de certificados:

- Plantillas de certificados versión 1.
- Plantillas de certificados versión 2.

Todas estas plantillas son almacenadas como objetos dentro del Directorio Activo y en la configuración del contexto de nombres como CN=*Certificate Templates*, CN=*Public Key Services*, CN=*Services*, CN=*Configuration*. Las plantillas de certificados están definidas para todo el bosque de dominio y pueden ser modificadas por un usuario con los permisos necesarios en cualquier computadora que tenga instalado MMC (Komar and Team, 2008)

2.6.1 Publicación de plantillas de certificados

Antes de que se realice la petición de un certificado es necesario que se encuentren disponibles las plantillas de certificados para su inscripción ante la CA. Para realizar la inscripción de las plantillas de certificados se debe trabajar desde la PC donde radica la CA como un miembro del grupo de administradores de la misma. En *Administrative Tools* \ *Certification Authority* \ *CAName* (nombre de la CA) *Certificate Templates* (menú contextual)*New**Certificate Template to Issue*\ *Enable Certificate Templates* y se habilitan todas las plantillas de certificados que se deseen publicar en la CA, quedando de esta manera disponibles para la inscripción. La lista de las plantillas de certificados publicadas quedan definidas en cada una de la CAs de la jerarquía, en dependencia de la disponibilidad de plantillas por nivel.

Si se desea eliminar una plantilla de certificados se realiza la operación manualmente o mediante el siguiente *script*, el cual permite agregar o eliminar estas plantillas automáticamente. *Name* corresponde al tipo de plantilla que se desea publicar

```
::Elimina plantillas de certificados.
certutil -SetCAtemplates -Administrator
certutil -SetCAtemplates -DirectoryEmailReplication
certutil -SetCAtemplates -DomainControllerAuthentication
certutil -SetCAtemplates -EFSRecovery
certutil -SetCAtemplates -EFS
certutil -SetCAtemplates -DomainController
```

certutil -SetCAtemplates -WebServer

certutil -SetCAtemplates -Machine

certutil -SetCAtemplates -User

certutil -SetCAtemplates –SubCA

:: Publica plantillas de Certificados

certutil -setCAtemplates + Name

Es necesario señalar que si se trabaja sobre un servidor de *Windows 2003 Enterprise Edition* ó *Data Center Edition* la versión de plantillas de certificados que se encuentra disponible es la 2; en caso que se tenga instalado un servidor de *Windows 2003 Standard Edition* la versión disponible será la 1.

2.7 Despliegue de certificados

Una vez implementada la jerarquía de autoridades certificadoras, según el modelo más conveniente para la red donde se pretenda implementar una PKI, se procede a realizar el análisis del despliegue de certificados a través de la misma.

Una petición de certificado implica que se comiencen a generar acciones tanto en la computadora desde donde se realizo la petición, como en la CA encargada de la generación y publicación del mismo. El proceso que toma lugar se muestra en la siguiente figura:

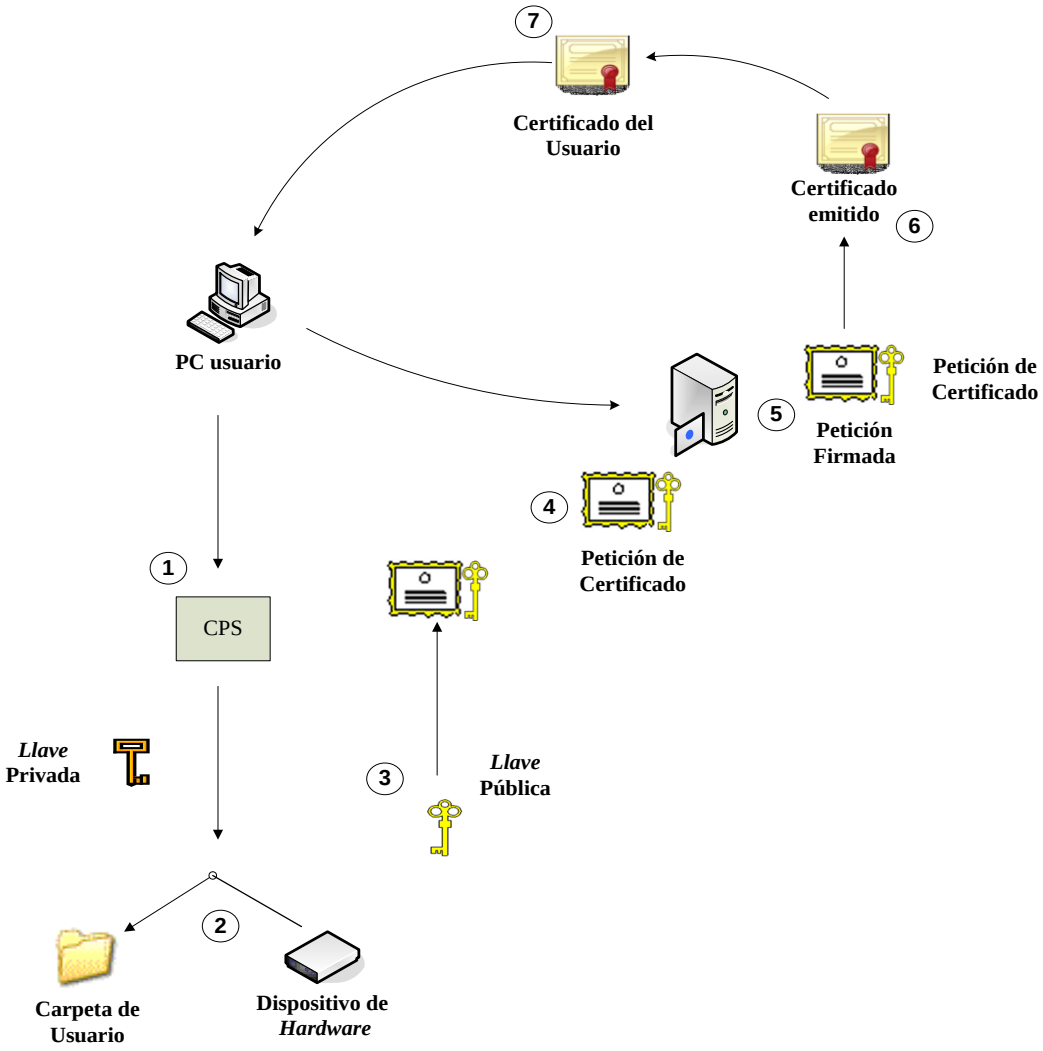

Figura 2.2 Despliegue de Certificados.

1. La computadora cliente pregunta por el abastecedor de servicio criptográfico (CPS) designado, por la plantilla de certificado o por el usuario, para generar el par de llaves.
2. El CPS genera un certificado basado en la longitud de la llave especificada en la plantilla de certificado o seleccionada por el usuario. Si el CPS es a base de *software* el par de llaves es generada en el perfil del usuario, si el CPS es a base de *hardware* (*smart card*), el par de llaves es generada en el dispositivo de *hardware*.
3. La llave pública del par de llaves es añadida a la petición de certificado junto con cualquier información requerida por la plantilla de certificado o por la configuración del usuario.

4. La petición de certificado es firmada por la llave pública del par de llaves y es enviada a la CA.
5. La CA publica el certificado solicitado, deniega la petición ó lo deja pendiente hasta que un administrador de la jerarquía manualmente apruebe o deniegue la petición.
6. El certificado es generado y firmado por la CA. El *hash* resultante el colocado en una base de datos.
7. El certificado publicado es devuelto al usuario y luego es almacenado en el perfil del usuario o en el dispositivo de *hardware* .El certificado ya es asociado con la llave privada del par de llaves y esta listo para usar.

2.8 Métodos de inscripción de certificados

Existen varios métodos de inscripción de certificados. Estos abarcan desde los métodos manuales que son inicializados por el usuario que realiza la petición del certificado; hasta los métodos automáticos donde la petición es iniciada por la Política de Grupo o por un *script* de entrada al sistema.

Para cada aplicación PKI permitida, se debe elegir el mejor modo de desplegar certificados a usuarios, computadoras, y dispositivos de red. En la mayor parte de los casos, se contará con un método primario y otro secundario.

La inscripción manual de certificados, no es un método práctico cuando se cuenta con una gran cantidad de usuarios, sobre todo por el tiempo que debe ser invertido en la preparación de personal calificado para la tarea. La auto inscripción por otra parte, disminuye el costo de una PKI, disminuyendo el tiempo y esfuerzo requerido para el despliegue de certificados.

2.8.1 Inscripción manual de certificados

La instalación de los Servicios de Certificados incluyen las Páginas de Inscripción *Web*, las cuales son accesibles solo si, también son instalados en la CA los Servicios de Información de Internet (IIS) (Komar and Team, 2008). Para realizar la petición de un certificado a las Páginas de Inscripción *Web* se accede al URL *http://CertServerDNS/certsrv*, donde *CertServerDNS* corresponde al nombre del dominio (DNS) donde se encuentra instalada la

autoridad certificadora (*http://uclv.edu.cu/certsrv*). Es importante recordar que antes de realizar este proceso los modelos de plantillas que se desean solicitar deben estar publicadas en la CA. En la página de Bienvenida se selecciona *Request a certificate*\ *Advanced Certificate Request*\ *Create and Submit a Request to this CA*. En la ventana de *Advanced Certificate Request* se deben definir las opciones siguientes para realizar la petición de certificados:

- ***Certificate template drop-down:*** Lista de las plantillas de certificados disponibles para realizar la petición.
- ***Key set*****:** Permite elegir entre la generación de un par de claves nuevas o utilizar un par existente para la creación del certificado.
- ***CSP drop-down*****:** Permite seleccionar un CPS instalado en la computadora cliente para realizar la petición de certificado.
- ***Key size*****:** Longitud del par de claves.
- ***Container name*****:** Archivo donde será almacenado el par de claves.
- ***Export options*****:** Permite solicitar la clave privada para exportarla.
- ***Strong key protection*****:** Requiere de una contraseña cada vez que el certificado tiene acceso a la clave privada.
- ***Store certificate in the local computer store***: Esta opción solo es permitida para certificados de computadoras y garantiza el almacenamiento local del certificado.
- ***Request format*****:** Permite elegir entre los formatos de Mensaje de Dirección de Certificado sobre *Cryptographic Message Syntax* (CMC) (Schaad and Myers, 2008) ó *Public Key Cryptography Standards* (PKCS) #10.
- ***Friendly name*****:** Nombre lógico asignado al certificado.

Una vez culminado el proceso de configuración se accede a *Submit*\ *Install this Certificate* y se espera la confirmación de que el certificado fue instalado con éxito.

Si la opción de *CA Certificate Manager Approval* de la plantilla de certificado es permitida en la etiqueta de emisión de certificados, entonces el certificado queda pendiente hasta que el gerente de la CA valide la petición. Para solicitar la validación del certificados se accede a *http://CertServerDNS/certsrv*\ *View the Status of a Pending Certificate Request*\ *pending*

certificate\ *Install this Certificate* y se espera la confirmación de que el certificado ha quedado instalado correctamente.

Otro de los métodos manuales de inscripción de certificados lo constituye el *Certificate Request Wizard*, herramienta que trabaja a través de *Microsoft Management Console* (MMC). El despliegue de esta opción consta de dos etapas: primero debe ser configurado el MMC con los ajustes necesarios y después se procede a la petición de certificados.

En el menú de archivos de MMC se selecciona *Add/Remove Snap-in*\ *Add*\ *Available Standalone Snap-ins*\ *Certificates*\ *Add.* En la nueva ventana de *Certificates Snap-in* si se desea solicitar un certificado de usuario la opción es *My User Account*, si el certificado es para una PC entonces se debe seleccionar *Computer Account.*

Cuando se tienen especificados correctamente los tipos de certificados que se van a configurar en la ventana *Certificates*, entonces se procede a la petición de los mismos mediante *Certificate Request Wizard*.

En el árbol de consola de *Certificate Request Wizard* se amplia *Certificates*\ *Current User* ó *Certificate* (*Local Computer*), luego se accede a *Personal*\ *Certificates* (menú contextual)*Personal* \ *All Tasks* \ *Request New Certificate*. De una lista limitada, en dependencia de los permisos que posea el usuario o la máquina local que solicita el certificado, se selecciona el tipo de certificado que se desea obtener. En *Certificate Friendly Name and Description* el usuario que realiza la petición, seleccionará un nombre (con carácter descriptivo) para el certificado. Luego de terminado el proceso, si la petición es aceptada se podrá observar el certificado en la ventana de detalles.

2.8.2 Generación automática de certificados

En cuanto a los métodos automáticos de inscripción de certificados podemos mencionar dos de ellos:

- ***Automatic Certificate Request Settings* (ACRS)**: aunque proporciona un método automático de distribución de certificados, presenta la limitante de que sólo las plantillas de certificado de la versión 1 pueden ser distribuidas y nunca a cuentas de usuarios. Aunque limitado ACRS es útil para distribuir certificados IPsec a todas las PC en el dominio (Cleveland, 2001). Para utilizar esta variante se accede a *Active*

Directory Users and Computers a través de *Administrative Tools*. Mediante las propiedades de la OU correspondiente al dominio se edita un nuevo objeto dentro del Grupo de Políticas. Luego en *Computer Configuration\Windows Settings\ Security Settings, \Public Key Policies\Automatic Certificate Request Settings* se realiza una nueva petición de certificados, especificándose que es para computadoras y finaliza el proceso.

- ***Autoenrollment Settings***: Los ajustes de auto-inscripción son una combinación de Políticas de Grupo y plantillas de certificados versión 2. Para permitir la auto-inscripción en una plantilla de certificado versión 2 se deben realizar ajustes, en *Security tab* para permitir la inscripción y autoinscripción de usuarios, computadoras o grupos a los cuales se le desea asignar un certificado; y en *Request Handling tab* para establecer el nivel de implicación que tendrá el usuario en el proceso de auto inscripción. Una vez que usted define las plantillas de certificado para ser desplegadas con la autoinscripción (*certtmpl.msc*), se pone en práctica la Política de Grupo que se encuentra ubicada en la OU donde se radica la cuenta del usuario o la computadora que va realizar la petición. En ambos casos el camino a seguir para realizar las modificaciones en el CP es *Computer Configuration* ó *UserConfiguration\WindowsSettings\SecuritySettings\PublicKeyPolicies\Autoenrollment Settings*. Las opciones de ajustes abarcan desde la inscripción automática hasta la revocación, actualización y eliminación de certificados

2.8.3 Certreq.exe

Otro medio para la inscripción de certificados es a través de la herramienta ***Certreq.exe***, la cual permite la creación de archivos que pueden presentar, recuperar y aceptar peticiones de certificados realizadas a la autoridad certificadora.

Los *scripts* utilizados en ***Certreq.exe*** para la inscripción de certificados son:

- ***Certreq –new Policyfile.inf RequestFile.req*:** crea un archivo de petición de certificado (*RequestFile.req*) basado en la configuración proporcionada en el archivo *Policyfile.inf*, la cual es mostrada a continuación.

  [NewRequest]

PrivateKeyArchive = FALSE

KeyLength = 1024

SMIME = TRUE

Exportable = TRUE

UserProtected = FALSE

KeyContainer = "..."

MachineKeySet = TRUE

Silent = TRUE

ProviderName = "Microsoft Enhanced Cryptographic Provider v1.0"

ProviderType = 1

UseExistingKeySet = TRUE

RequestType = PKCS10

KeyUsage = 0x80

[RequestAttributes]

CertificateTemplate=User

- **_Certreq –submit –config CADNSName\CALogicalName RequestFile.req_:** Presenta el archivo de petición de certificado a la autoridad certificadora y devuelve la identificación de la petición presentada.
- **Certreq –retrieve –config _CADNSName\CALogicalName RequestID_:** Recupera el certificado publicado de la autoridad certificadora. El certificado recuperado es almacenado en el sistema de archivo local *Certfile.cer*.
- **Certreq –accept _Certfile.cer_:** Vincula el certificado con la llave privada generada durante la creación del archivo de petición de certificados

2.9 Políticas de seguridad

Una jerarquía de autoridades certificadoras es tan segura como las medidas que se tomen para protegerla. Normalmente este grupo de medidas se clasifican en medidas de seguridad a partir de la configuración de CAs y en medidas de seguridad físicas.(Lee et al., 2006)

Las medidas de seguridad a partir de la configuración de las CAs se refieren a las implementadas en la configuración de los servicios de certificados o en la configuración de *Windows Server 2003*. Estas medidas incluyen:

1. Definición de plantillas de seguridad tanto para CA autónomas, como para las que se encuentran conectadas en línea.

Los ajustes que deberían ser considerados para la inclusión en una plantilla de seguridad de CA son:

- Deshabilitar servicios innecesarios.
- Definir grupos restringidos.
- Asignar derechos de usuario.
- Realización de Auditorias.

2. Habilitar todas las opciones de revisión en las propiedades de las autoridades certificadoras.

Cuando se habitan todas las opciones de auditorias se asegura que todos los eventos importantes relacionados con las operaciones del los Servicios de Certificados quedan registrados en el *Security Log* de *Windows*.

3. Restringir los miembros en el grupo de administradores locales.

Cuando se instala una autoridad certificadora utilizando cualquier CPS la llave privada de la misma queda almacenada en una base de datos local, por lo que restringiendo el número de administradores locales, se limita el número de de usuarios con probabilidades de comprometer dicha llave.

4. Hacer cumplir la separación de roles.

La separación de roles por criterio común (*Common Criteria*) garantiza que un usuario pueda desempeñar solo uno de los papeles siguientes dentro de la PKI: Administrador de CA, Manejador de Certificados, Auditor y Operador de Salvas. La asignación de dos o más de esto roles causa que al usuario le sean denegadas todas las acciones de administración de la CA.

5. Deshabilitar el *Terminal Server* en la computadora donde radica la CA.

De esta manera se imposibilita el manejo de la CA mediante un acceso remoto, situación que comprometería el desempeño de la PKI.

Como complemento de las medidas de seguridad de configuración de la CA se deben poner en práctica medidas de seguridad físicas como las siguientes:

1. Almacenar las computadoras de las autoridades certificadoras autónomas y sin conexión en un cuarto físicamente asegurado.
2. Almacenar las computadoras de de las autoridades de certificación en una caja de seguridad.
3. Mantener la base de datos de *hardware* (disco duro) de las autoridades de certificación separadas y almacenadas en un lugar seguro.
4. Deshabilitar la entrada por hardware en el BIOS de la computadora donde radica la autoridad certificadora.
5. habilitar la entrada por contraseñas al BIOS de las autoridades certificadoras autónomas.
6. Implementar *SYSKEY* de nivel dos o tres.

CAPÍTULO 3 PROPUESTA DE CONFIGURACIÓN DE LOS NIVELES DE SEGURIDAD DE LOS SERVICIOS INTEGRADOS A LA PKI.

3.1 Metodología para la implementación

Para profundizar en los niveles de implementación de una infraestructura de Llave Pública aplicada al entorno de la Intranet de la UCLV, que permita lograr completa interoperabilidad e integración a las principales aplicaciones y servicios existentes es de vital importancia seguir una estrategia que permita obtener resultados exitosos. Esto incluye analizar los requerimientos de la institución y realizar un correcto planeamiento para su despliegue lo que implica una ejecución consecuente de las tareas (Crespo, 2008).

El procedimiento que se empleará consta de los pasos siguientes: análisis de los requerimientos de la institución, diseño e implementación de la arquitectura y de las operaciones. Luego se procederá a la integración y despliegue de los servicios.

3.2 Características de la Intranet de la UCLV

La Intranet de la Universidad Central "Marta Abreu" de Las Villas cuenta con alrededor de 3139 computadoras (no todas en red, déficit de *switch*) repartidas entre facultades, centros de investigación y administrativos. En general, está compuesta por dominios físicos *Ethernet* 100BASET interconectados en una *Gigabit Ehternet* por medio de un *backbone* de fibra óptica con topología estrella.

En la actualidad se encuentra interconectada a las redes de otras universidades del país, a las 14 Sedes Universitarias Municipales (enlaces a 64 Kbps) y a la Escuela de Trabajadores Sociales, de lo cual resultó una gran red del Ministerio de Educación Superior. El esquema de direccionamiento escogido para este ministerio es clase A para redes privadas 10.0.0.0/8. A la Intranet de la UCLV le fue otorgada la dirección 10.12.0.0/16, la cual se encuentra dividida en varias subredes. El espacio de nombres de dominio asignado es el UCLV.EDU.CU.

Los servicios más importantes brindados por la Intranet son correo electrónico, acceso a Internet y sistema de control docente, los cuales están ubicados en el nodo principal (La Puerta) con el objetivo de homogeneizar y centralizar la gestión de los sistemas y servicios

más importantes, establecer relaciones de confianza entre los dominios y suministrar condiciones óptimas de *hardware* así como respaldo eléctrico. Las cuentas de los usuarios (10985 cuentas de usuarios) también son administradas centralmente para mayor estabilidad. (Crespo, 2008).

Todos los dominios de la Intranet se encuentran implementados sobre *Windows Server 2003* y la mayoría de los servicios fundamentales y las computadoras personales están soportados sobre algún sistema operativo perteneciente a *Microsoft.* En muchos servidores y dependencias investigativas podemos encontrar otros sistemas operativos, casi todos pertenecientes a la familia Linux como *Debian*, *Red Hat*, *Ubuntu* y *Gentoo*.

3.2.1 Principales vulnerabilidades

En la Intranet de La UCLV la forma de autentificación de los usuarios son las contraseñas. Él mecanismo ha demostrado ser práctico y sencillo para el usuario; pero aunque cuenta con protocolos de autentificación de gran fortaleza (principalmente *Kerberos)*, su seguridad es dudosa debido al alto grado de desarrollo alcanzado por los *crackers* de contraseñas los cuales pueden, con el poder de cómputo actual, obtener cualquier contraseña que el ser humano sea capaz de memorizar (Jung and Jung, 2006).

En la Intranet no están habilitadas otras formas de autentificación. Mecanismos vinculados a la criptografía tales como certificados y firma digital para la protección de los sistemas de archivos, el correo electrónico y el establecimiento de relaciones de confianza entre los usuarios de la Intranet, no se encuentran implementados.

Por otra parte tampoco se cuenta con una infraestructura propiamente dicha que actúe como móvil para soluciones más fiables, sirva para sostener un modelo de confianza mucho más robusto y brinde múltiples servicios de seguridad. (Crespo, 2008)

3.3 Legislaciones

Corresponde al Ministerio del Interior autorizar el diseño, producción y comercialización de sistemas de protección criptográfica y prestación de estos servicios a órganos, organismos y entidades estatales. , según el Artículo 39, Capítulo IV del Decreto-Ley Nº 199 Sobre la Seguridad y Protección de la Información Oficial.

3.4 Preparación del Directorio Activo

Al encontrarse todos los dominios de la Intranet soportados sobre *Windows Server* 2003 la implementación de una PKI sobre este sistema operativo no requiere la creación de un nuevo dominio o que se realicen cambios significativos en el bosque de nombres de dominio. La única modificación que es necesario realizar es referente a los grupos de Publicadores de Certificados (*Cert Publishers*) presentes en el Directorio Activo. En los servidores de *Windows* 2003 los Publicadores de Certificados son un grupo de dominio local que están presentes en cada dominio del bosque; para que una CA pueda emitir certificados a cualquier objeto del bosque o se pueda poner en contacto con objetos pertenecientes a otro bosque su cuenta debe ser añadida al grupo de Publicadores de Certificados de cada dominio de la Intranet.

3.5 Codificación SSL para servidores *web*

La búsqueda de archivos dentro de la Intranet es una de las aplicaciones mas comúnmente usadas en la UCLV. EL Protocolo de Transferencia de Hipertexto (HTTP) por defecto no emplea codificación de datos para transferencias entre el servidor *web* y los usuarios que tienen acceso a él(2006). Un servidor *web* que tenga un certificado *web* instalado, puede implementar el protocolo de codificación *Secure Sockets Layer* (SSL) (Chandra et al., 2003), garantizándose de esta forma la validación por parte de los usuarios del sitio *web*, del certificado del servidor para comprobar su identidad; y la codificación de los datos que viajen entre ambos (Raina, 2003).

Cuando se implementa SSL se deben identificar los certificados que permitan habilitar codificación entre el servidor *web* y sus usuarios. Dos tipos de certificados pueden ser usados (Piñón and Camacho, 2007):

1. **Certificado de servidor *web***: un certificado de servidor de *web* es obligatorio cuando se implementa SSL en un servidor *web*. Este tipo de certificados brinda codificación a los mensajes procedentes de un usuario y permite la validación del certificado del servidor para demostrar la identidad del mismo.
2. **Certificado de usuario *web***: Cuando un sitio *web* necesita la identificación de un usuario que desea acceder a él, el usuario puede utilizar un certificado basado en

autenticación. Este tipo de certificado no requiere necesariamente de SSL, pero si este protocolo se encuentra implementado, las credenciales del usuario se encontraran mejor protegidas.

Otra consideración de importancia en la implementación de SSL es la búsqueda de un abastecedor de certificados confiable para obtener el certificado del servidor *web*. Normalmente esta decisión se basa en las categorías de los usuarios que acceden al servidor, estos pueden ser internos o externos. Los usuarios internos pertenecen a la organización y tienen una cuenta en la red de la misma; por otra parte los usuarios externos no pertenecen a la organización ni poseen una cuenta de usuario dentro de la misma, pero en algún momento, han establecido contacto con el servidor *web*.

Una organización decide publicar certificados de servidor *web* de una CA privada cuando desea hacer cumplir sus políticas de seguridad y necesita reducir el los gastos asociados a la publicación de certificados de servidor *web* a usuarios externos

3.5.1 Publicación de certificados de servidor *web*

El proceso de petición y publicación de un certificado de servidor *web* varía según el tipo de dispositivo desde el cual es generada la petición. Las opciones de publicación de certificados de una *Enterprise CA* incluyen:

1. Certificados de servidores *web* que tienen implementado *Internet Information Services* (IIS) en computadoras miembros del bosque de dominio.
2. Certificados de servidores *web* que tienen implementado IIS en computadoras que no son miembros del bosque de dominio.
3. Certificados de servidores *web* para terceros o aceleradores de red mediante dispositivos de hardware.

Cuando se publica un certificado de servidor *web* se utiliza el *Web Server Certificate Wizard* y la petición de certificado es presentada en el contexto de seguridad del usuario que utiliza esta herramienta. Este usuario debe ser administrador local del servidor *web*, asi como tener permisos de lectura y despliegue de plantillas de certificados para archivar certificados en la base de datos de la máquina.

La instalación del certificado del servidor *web* consta de dos pasos:

1. Se realiza la petición y se instala el certificado de servidor *web* en el servidor.
2. Se configura el servidor *web* para permitir codificación SSL en un sitio *web* o en un servidor virtual.

3.5.2 Petición e instalación de certificados de servidor *web*

La petición e instalación de un certificado de servidor *web* se realiza en *Windows Server 2003* desde la consola de administración de IIS. Para instalar un certificado se accede desde el menú de inicio a *Programs*\ *Administrative Tools*\ *Internet Information Services (IIS) Manage*r; en el árbol de la consola se expande *ServerName**Default Web Site* (menú contextual)\ *Properties*\ *Directory Security*. En la pestaña *Directory Security* se despliega la sección *Secure Communications*\ *Server Certificate*. En *Web Server Certificate Wizard* se va a la siguiente ventana: *Server Certificate*\ *Create a New Certificate*\ *Send the Request Immediately to an Online Certification Authority*. Enviando la petición de certificados a la CA, esta determina si publicar o denegar la petición del certificado basándose en los permisos asignados a la plantilla de certificado del servidor *web*. En la ventana de *Name and Security Settings* se da un nombre y una descripción del servidor *web*, así como se determina la longitud del mismo (1024 *bits*). En *Available Providers* se elige CSP, en *Organization Information* se especifica el nombre de la organización y del departamento; y en *Your Site's Common Name* se introduce el nombre del DNS (*eli.uclv.edu.cu*). El nombre del país, el estado y la ciudad son necesarios en la información geográfica. Si se tiene instalado IIS versión 6.0 se acepta el puerto (TCP 443) que viene definido por defecto para SSL. En *Choose a Certification Authority* se despliega la lista de autoridades certificadoras y se selecciona *Enterprise CA*. En *Certificate Request Submission* se verifican los ajustes y en *Completing the Web Server Certificate Wizard* se finaliza el proceso. El certificado es instalado en la base de datos local y puede ser utilizado por IIS.

3.6 Habilitando SSL en un servidor *web* IIS

Una vez que ha sido instalado el certificado del servidor *web* se implementa SSL para asegurar la comunicación con sitios *web*. Para realizar este proceso se accede *a Internet Information Services (IIS) Manager*, en el árbol de la consola se despliega el menú contextual del sitio *web* o el directorio virtual donde se va a habilitar SSL y se buscan sus

propiedades. Luego en la pestaña de *Directory Security* se accede a la sección *Secure Communications\ Edit*. En la nueva ventana de *Secure Communications* se habilita *Require Secure Channel (SSL)* y se permite una casilla de verificación de la información de 128 *bits*, culminándose así la operación.

Además de la codificación SSL, un servidor *web* brinda servicios de autenticación basados en certificados. En vez de la credenciales comunes o de estar conectado anónimamente al servidor *web*, un usuario puede elegir un certificado de su base de datos para autenticación mediante el *Client Authentication Enhanced Key Usage (EKU)*. El certificado tiene que ser asociado a una cuenta de la base de datos de cuenta de usuarios disponibles en IIS por un proceso conocido como correlación (*mapping*). Existen dos tipos de correlación:

1 **Correlación implícita**: traza un camino desde las propiedades de la cuenta del usuario en el Directorio Activo hasta la base de datos de correlación del IIS.
2 **Correlación explícita:** traza el camino del certificado a una cuenta de usuario basada en la información incluida en los campos de *Subject* y *Subject Alternate Name*.

Independientemente del método de correlación utilizado para asociar el certificado a una cuenta de usuario, dicho usuario bebe tener acceso a la llave privada del certificado para demostrar su identidad.

El IIS puede usar el Directorio Activo como su directorio de correlación con la ventaja de que así, la correlación estará disponible para múltiples servidores *web* siempre y cuando pertenezcan al dominio y puede ser utilizado en otras aplicaciones además del navegador *web*.

Para permitir a IIS usar correlaciones del Directorio Activo se debe:

1. **Crear una plantilla de certificado para la autenticación del usuario**: Para que un certificado permita a un usuario autenticarse en un navegador *web*, este debe utilizar firma digital e incluir un OID de autenticación de cliente (1.3.6.1.5.5.7.3.2).
2. **Definir las correlaciones en el Directorio Activo**: Si el certificado es publicado por una *Enterprise CA* perteneciente al bosque de dominio, entonces dicho

certificado contiene el UPN (*User Principal Name*) del usuario en el campo de *Subject Alternative Name* y es incluido en la base de datos *NTAuth* del Directorio Activo, permitiendo el uso de correlaciones implícitas.

Es necesario verificar que el certificado está incluido en la base de datos *NTAuth* del Directorio Activo, para realizar esta operación se accede a la herramienta *PKI Health Tool* (*pkiview.msc*) del *Resource Kit Tools.* En el árbol de consola se accede a *Enterprise PKI* (menú contextual)\ *Manage AD Containers*\ *NTAuthCertificates* y se verifica si el certificado se encuentra en la base de datos. De no encontrase, mediante *Add* puede ser añadido a esta.

3. **Permitir a IIS usar correlaciones de certificados**: El siguiente paso es configurar IIS para permitirle utilizar correlación basada en certificados. Para este procedimiento luego de abrir el *Internet Information Services (IIS) Manager*, se accede en el sitio *web* o el directorio virtual donde se desea habilitar la autenticación por certificados a *Properties**Directory Security*\ *Secure Communications*\ *Edit*. En la ventana de *Secure Communications* se deben especificar los siguientes ajustes:
   - ***Require secure channel* (*SSL*):** Habilitar.
   - ***Require client certificates*:** Seleccionar. Esta opción refuerza la autenticación basada en certificados mediante la configuración de métodos alternos de autenticación.
   - ***Enable client certificate mapping***: Habilitar**.**
4. **Habilitar el servicio de correlación del directorio**: Luego de permitir las correlaciones para sitios *web* o directorio virtual, es necesario habilitar el servicio de correlación de directorio de *Windows.* En el árbol de la consola de *Internet Information Services Manager* se accede a *Web Sites* (menú contextual)\ *Properties*\ *Directory Security*; en la nueva ventana se habilita *Windows Directory Service Mapper* y se concluye el proceso.

Configurar IIS para el uso de correlaciones de certificados IIS.es un proceso similar a la configuración de IIS para utilizar al Directorio Activo como directorio de correlación, la única diferencia es que no es necesario habilitar el servicio de correlación de directorio de

Windows

3.6.1 SSL para la Intranet UCLV

Dentro de la Intranet de la UCLV existen páginas *web* (Página de *Nagios*) cuya gestión de autenticación podría fortalecerse y simplificarse considerablemente con la integración de PKI y codificación SSL. El método actual de autenticación de usuarios (contraseñas) podría ser sustituido por certificados digitales, delegando el uso de contraseñas para otorgar privilegios en los diferentes niveles de acceso a la información, luego se utilizaría codificación SSL en la protección de estas contraseñas.

Otra variante que podría ser utilizada en el proceso de distinción de usuarios, con elevados perfiles de seguridad, sería publicar plantillas de certificados con permisos diferentes para la autenticación de usuarios

3.7 Correo electrónico seguro

El Correo Electrónico constituye el principal medio de comunicación entre usuarios de la Intranet. Debido a su configuración inicial los paquetes de correo viajan sin codificación alguna, por lo que es factible para un atacante tener acceso a la información mientras esta se mueve a través de la red. Una Infraestructura de Llave Pública permite aplicar al correo electrónico medidas criptográficas para garantizar su seguridad (Kambourakis et al., 2007).

Dos métodos son puestos en práctica para asegurar el correo electrónico:

1. **Asegurar el contenido del mensaje:** el contenido del mensaje es asegurado implementando *Secure/Multipurpose Internet Mail Extensions* (S/MIME), el cual permite a programas de correo electrónico, brindar tanto servicios de firma digital como de codificación. (Kuzmowycz, 2001)
2. **Asegurar los datos cuando viajan por la red:** el flujo de datos se protege implementando *Secure Sockets Layer* (SSL) o *Transport Layer Security* (TLS), que proporcionan validación de identidad cuando el mensaje viaja desde el servidor hasta el destinatario. TLS y SSL tienen ligeras diferencias, pero el protocolo en sí es esencialmente el mismo (Dierks and Rescorla, 2006)

3.7.1 SSL para protocolos de correo electrónico

Además de firmar digitalmente y codificar los mensajes de correo electrónico, se puede aumentar la seguridad de autenticación mediante los protocolos de Petición de Comentario (*Request for Comment*- RFC) soportados por *Microsoft Exchange Server 2003*. Alguno de estos protocolos se describen a continuación:

1 ***Post Office Protocol 3*** **(POP3):** permite recuperar mensajes del buzón de entrada de un usuario en un servidor de correo electrónico.
2 ***Internet Message Access Protocol 4*** **(IMAP4):** Permite recuperar cualquier mensaje que se encuentre almacenado en un servidor de correo.
3 ***Simple Mail Transfer Protocol*** **(SMTP):** Se utiliza para enviar mensajes a recipientes de correo electrónico.
4 ***Network News Transfer Protocol*** **(NNTP):** Se utiliza para descargar mensajes de grupos de noticias.

Ninguno de estos protocolos codifica la información cuando transmite los datos entre el cliente y el servidor, por lo que si un atacante capturara con un *sniffer* la cadena de datos, podría leer sin grandes impedimentos, el mensaje que contiene. Mediante la implementación de SSL se protegen los datos cuando viajan entre el cliente de correo electrónico y el servidor. Cuando SSL es implementado, la comunicación se establece a través de los puertos que se muestran en al tabla 3.1

Protocolo	Puertos por defecto	Puerto SSL
POP3	TCP 110	TCP 995
IMAP4	TCP 143	TCP 993
SMTP	TCP 24	TCP 24 ó 465
NNTP	TCP 119	563

TABLA 3.1

Para habilitar SSL en *Microsoft Exchange Server 2003,* el servidor debe tener instalado un

certificado que incluya el OID de *Server Authentication Enhanced Key Usage* (EKU), similar a un certificado de un servidor *Web*. Se utiliza el mismo certificado para cada uno de los protocolos.

3.7.2 Habilitar certificado de servidor *web* para correo electrónico

La instalación de este certificado debe realizarse en un servidor de correo como un usuario perteneciente al grupo de administradores. Desde el menú inicio se accede a *All Programs*\ *Microsoft Exchange*\ *System Manager*. En la nueva ventana se despliegan a las siguientes opciones: *Servers**ComputerName* (nombre del servidor de correo)*Protocols**RFCProtocol* (nombre del protocolo, ejemplo POP3)*Default RFCProtocol Virtual Server* (menú contextual)\ *Properties*\ *Certificate*\ *Create a New Certificate.* Si ya se tiene un certificado instalado en el servidor *web* se selecciona la opción de *Assign an Existing Certificate*. Para continuar con la instalación en la ventana *Delate or Immediate Request* se accede a *Send the Request Immediately to an Online Certification Authority*, asumiéndose que la petición de certificado se le realiza a una empresa de autoridades de certificación (*Enterprise CA*) y no a una autoridad independiente *(Standalone CA),* de ser este último el caso se debe guardar la petición en un archivo de petición. En *Name and Security Settings* se acepta el nombre y la longitud del mismo que aparece por defecto. En la ventana de *Your Site's Common Name* se especifica el nombre del DNS que se utiliza para conectarse al servidor de correo. En la información geográfica se especifica la localidad, la zona y el país donde radicara el servidor de correo y se selecciona una autoridad de certificación de la lista despegable para dar por finalizado el proceso (Komar and Team, 2008).

3.7.3 SSL para protocolos RFC

Una vez que el certificado *web* es instalado se procede a habilitar SSL para un protocolo RFC. El camino a seguir es *Default RFCProtocol Virtual Server* *Properties**Communication*, habilitándose en la ventana de *Security* la opción de *Require Secure Channel*\ *Require 128-Bit Encryption*.

Habilitar SSL en un *Exchange Server* en algunos casos requiere modificaciones en el *firewall* del servidor, para permitir que se establezca comunicación con los puertos SSL.

Para la Intranet de la UCLV es recomendable que todos los usuarios implementen codificación SSL, sobre todo para aquellos que posean privilegios de seguridad elevados (administradores de red). Es importante para este último grupo de usuarios proteger sus mensajes cuando viajan por la red, de forma tal, que información confidencial no pueda ser utilizada con fines de chantaje o para técnicas de ingeniería social.

3.7.4 Elección de Autoridades de certificación

Para implementar correo electrónico seguro utilizando S\MIME, el primer paso será decidir donde adquirir el certificado S\MIME correspondiente (Santesson, 2005). Estos certificados se pueden obtener tanto de una autoridad certificadora comercial, como de una privada.

Comúnmente los certificados S\MIME de usuarios, procedentes de una CA comercial se solicitan cuando la mayoría de los correos asegurados con S\MIME son enviados a usuarios fuera de la organización. La utilización de un certificado publicado por un abastecedor comercial como ***VeriSign*** en el que confían la mayor parte de las organizaciones, aumenta la probabilidad de que un usuario no perteneciente a la organización confíe en la firma digital asociada al certificado de la CA comercial.

Los certificados procedentes de CAs privadas se utilizan cuando la mayoría del correo electrónico asegurado con S\MIME, viaja entre usuarios de una misma organización. Como todos los usuarios confían en la CA raíz, entonces confían también en la firma digital y los procesos de codificación asociados a la misma. No es necesario gastar recursos en publicar certificados S\MIME privados para generar confianza.

Existen casos donde un usuario adquiere dos juegos diferentes de certificados S\MIME, uno para uso interno y otro para uso externo. Si el *software* de correo utilizado es *Outlook*, se puede crear dos perfiles separados para enviar correo electrónico. Estos perfiles designan que tanto el certificado de la CA privada como el de la CA comercial sean utilizados para los procesos de firma digital y codificación de la información. Ambos perfiles tienen acceso al mismo *Exchange Server*, pero cada uno define una combinación de certificados diferentes para transacciones S\MIME.

3.7.5 Elección de plantillas de certificados

Para desplegar plantillas de certificados de correo electrónico se debe definir si se desea utilizar el mismo certificado para firma digital y codificación o si se van a utilizar certificados diferentes. La ventaja de un solo certificado es que se simplifica el manejo de del mismo por parte de los usuarios, en todas las operaciones de correo electrónico; la desventaja de tener un único certificado consiste en que, si se implementan archivos de llaves del certificado del correo electrónico otro usuario podría ganar el acceso a la llave privada utilizada en todos los procesos.

Por otra parte dos certificados independientes posibilitan que el certificado que asume todas las operaciones de codificación pueda ser archivado sin que la firma digital se vea afectada.

3.7.6 Certificados combinados e independientes de correo electrónico

Cuando se va a utilizar un solo certificado para correo electrónico es recomendable crear una plantilla de certificado versión 2 basada en *Exchange User* ó *Exchange Signature Only*. Las opciones a configurar son las siguientes:

1 ***General*:** Se garantiza que el certificado sea publicado en el Directorio Activo y se define el período de validez y de renovación del mismo.
2 ***Request Handling*:** Se varía el propósito del certificado para que permita tanto firma digital como codificación. Otras opciones que pueden ser habilitadas son ***Key archival,*** que archiva una copia criptografiada de la llave privada del certificado en la base de datos de la CA; y ***Private key protection*** la cual protege la llave privada mediante la introducción de una contraseña.
3 ***Subject name*:** Permite autenticar al usuario desde la información almacenada en el Directorio Activo. Por propósitos S\MIME el certificado debe incluir la dirección de correo electrónico del usuario.
4 ***Security*:** En el grupo global que contiene todos los usuarios autorizados a firmar digitalmente se le debe agregar permisos para la codificación. Esta combinación de permisos permitirá el despliegue de certificados a usuarios utilizando autoinscripción.

Debido a los riesgos de implementar el archivo de llave privadas para el correo electrónico

con un solo certificado, se recomienda poner en práctica certificados separados para firma digital y codificación, garantizándose así que solo la llave privada asociada a la codificación del correo electrónico es archivada (Cross and Ben-Menahem, 2004).

Para un certificado independiente de firma digital se debe duplicar la plantilla de certificado basado en *Exchange Signature Only*. Cuando se separan ambos certificados se puede elegir desplegar el certificado de la firma digital en una tarjeta inteligente (Raina, 2003).

En el proceso de duplicar la plantilla de certificado, la configuración es muy similar al certificado combinado, introduciéndose solamente algunos cambios en:

1. ***General:*** Es recomendable no permitir la publicación del certificado en la casilla de verificación del Directorio Activo, pues un usuario no necesita descargar un certificado para comprobar la autenticidad de la firma digital dado que el mismo es incluido en la carga útil del mensaje.
2. ***Request Handling:*** Los ajustes recomendados en el despliegue de un certificado en una *smart card* (Hamann et al., 2001) radican en :
    1. ***Purpose***: Firma y entrada al sistema de *smarts card.*
    2. ***Prompt the user during enrollment***: Permitido.
    3. ***CSP***: *Microsoft Enhanced Cryptographic Provider v1.0*.

Por otra parte, desplegar el certificado de la firma digital del correo electrónico como un certificado almacenado en el perfil de usuario, requiere los ajustes siguientes en el ***Request Handling:***

1 ***Purpose***: Firma.

2 ***Allow Private key to be exported***: Esta opción es habilitada o deshabilitada, en dependencia de si se desea exportar o no, la llave privada del certificado de la firma digital.

3 ***Prompt the user during enrollment and require user input when the private key is used:*** Permitida.

4 ***CPS***: Se selecciona el proveedor de *smart card*.

Cuando se pone en práctica un certificado separado de codificación de correo electrónico se debe realizar un duplicado de las plantillas de certificados basados en *Exchange User.*

Los campos de configuración de estas plantillas de certificados son similares al certificado combinado, estableciéndose solamente cambios en la opción ***General*** y en ***Request Handling.***

En ***General*** se verifica que la publicación del certificado se realizará en la casilla de verificación del Directorio Activo, de modo que otros usuarios puedan recuperar el certificado de codificación de usuario del catálogo general y en ***Request Handling*** deben quedar definidos los siguientes ajustes:

1 ***Purpose:*** Codificación.
2 ***Archive subject's encryption private key***: Permitido.
3 ***Include symmetric algorithms allowed by the subject***: Permitido.
4 ***Allow private key to be exported*****:** Permitido.
5 ***Prompt the user during enrollment and require user input when the private key in use***: Permitido.
6 ***CSP:*** *Microsoft Enhanced Cryptographic Provider v1.0*.

3.7.7 Métodos de despliegue

La autoinscripción es el método mas recomendado para desplegar plantillas de certificados, permitiendo la inscripción automatizada a los certificados de correos electrónico a todos los usuarios miembros del dominio cuyas computadoras soporten *Windows* XP.

Entre los métodos de autoinscripción se encuentran:

1 **Inscripción *Web***: Un usuario que pertenezca al dominio puede utilizar las Páginas de Inscripción *Web* de Servicio de Certificados.
2 ***Scripts* de inscripción a certificados de firma digital**: El *script enroll.vbs* (ver *\\10.12.57.1\tesis$\Elisabeth PKI en la intranet de la UCLV\CD PKI PKI.And.Certficate.Security\Enroll Script*) automatiza la petición de un certificado para firma digital de correo electrónico. El usuario debe dirigir el *script* utilizando una línea de comando con la sintaxis *cscript enroll.vbs /ca "issuingca.uclv.edu.cu\Intranet UCLV Issuing CA" /certtype EmailSign /keyl 1024 /csp enhanced*.

3.7.8 Habilitando correo electrónico seguro

Una vez que los certificados han sido desplegados con éxito, cada usuario debe configurar su aplicación de correo electrónico para utilizar S\MIME (Komar and Team, 2008)

- ***Outlook***

Tanto *Outlook* 2002 como *Outlook* 2003 usan firma digital y codificación de correo electrónico, solo se debe garantizar que los certificados se encuentran disponibles en el perfil de usuario. Se puede verificar la existencia de los certificados y crear algoritmos para la firma digital y la codificación accediendo a *Outlook* \ *Tools*\ *Options*\ *Security*\ *Settings.* En la ventana de *Change Security Settings* se debe asegura que los ajustes siguientes son definidos:

1. ***Cryptography Format***: S/MIME.
2. ***Default Security Settings for this cryptographic message format***: Permitido.
3. ***Default Security Settings for all cryptographic messages***: Permitido.
4. ***Hash Algorithm***: SHA1 ó MD5 (es recomendado SHA1).
5. ***Encryption Algorithm***: 3DES, RC2 (128-bit), RC2 (64-bit), DES, RC2 (40-bit). Se recomienda 3DES.
6. Se habilita la opción de enviar los certificados con los mensajes firmados.

- ***OWA***

Para permitir el uso de S\MIME en *OWA* se debe instalar en la computadora del usuario *S/MIME ActiveX*, *software* que permite el uso de este protocolo en la firma y codificación de mensajes de correo electrónico.

La instalación de *S/MIME ActiveX* se realiza por un administrador local de la máquina. En el explorador de Internet se accede a *http://uclv.edu.cu/OWA*. El usuario se autentifica para tener acceso al recipiente de mensajes, en *Outlook Web Access*\ *Navegación*\ *Options*\ *E-Mail Security* (bajo)\ *Download*, cuando se intente abrir el archivo descargado debe aparecer una advertencia de seguridad, esta advertencia confirma la instalación del *ActiveX*

Una vez que se ha implementado S\MIME en el paquete de correo electrónico, la decisión de utilizar firma digital o codificación esta en manos del usuario

- ***Outlook Express***

Outlook Express no asigna automáticamente el uso de certificados para S\MIME, por lo el usuario debe modificar las propiedades de su existencia POP3 ó cuenta de correo IMAP, para seleccionar los certificados de correo electrónico seguro. Para configurar la firma y codificación de correo electrónico se accede desde el menú de inicio a *All Programs*\ *Outlook Express* donde se deshabilita la opción que aparece por defecto al acceder a *Outlook Express* como un cliente de correo electrónico. Luego en *Tools*\ *Accounts*\ *Mail**POP3 ó IMAP**Properties**Security**Signing Certificate**Select* se selecciona S\MIME para certificado de firma digital. Una vez que se realiza dicha operación se recorre un nuevo camino *Properties*\ *Security*\ *Encrypting Preferences*\ *Select* para habilitar S\MIME para el certificado de codificación. Antes de culminar el proceso se debe elegir de la lista desplegable de algoritmos, el algoritmo de codificación que se va a utilizar.

Por políticas de seguridad de la Intranet *Outlook Express* solo esta habilitado para conexiones telefónicas (lenta transferencia de datos). En este caso no tiene sentido configurar correo electrónico para el uso de certificados en el proceso de cifrado de la información dado que la comunicación se establece solamente entre dos estaciones de trabajo, pero sin embargo seria útil únicamente para el proceso de autenticación.

3.8 Redes inalámbricas

Muchas organizaciones implementan y experimentan con redes inalámbricas, la Universidad Central de las Villas es una de ellas. Las redes inalámbricas tienen la ventaja de aumentar la movilidad de un usuario en un espacio geográfico determinado, permitiéndole mantener conectividad con la red. Con las redes inalámbricas surgen varias amenazas que no existían con las redes cableadas (Komar and Team, 2008). Dentro de estas amenazas tenemos:

1 Uniones casuales a la red inalámbrica.
2 Fácil inspección e intersección de datos.
3 Modificación de datos mediante ataques “hombre en medio”.
4 Uniones a la red no autorizadas.

Cuando se implementa una red inalámbrica se debe elaborar un plan para reducir la probabilidad de que ocurran algunas de estas amenazas. Entre los principales métodos

tenemos el Filtrado MAC, la Privacidad Equivalente a Conexión (WEP) y el Acceso Protegido Wi-Fi (WPA) (Satizábal et al., 2007). La autenticación 802.1x es uno de los métodos incluidos dentro de WPA para garantizar la conectividad a la red inalámbrica solo a usuarios ó computadoras autorizados.

Una PKI en *Windows Server 2003* proporciona los certificados necesarios para la autenticación 802.1x tanto en redes conectadas como inalámbricas. Cuando un usuario ó computadora trata de conectase a una red, dos tipos de autenticación se encuentran disponibles (Goffee et al., 2004a):

1. ***Extensible Authentication Protocol with Transport Layer Security (EAP/TLS)*:** Es un método de autenticación mediante certificados que permite la autenticación mutua entre un usuario o computadora y el servidor de Servicio de Marcación Interna de Autenticación Remota de Usuario (RADIUS). Para implementar la autenticación EAP/TLS son necesarios certificados de autenticación de computadoras, usuarios y servidores. (Nakhjiri and Nakhjiri., 2005)
2. ***Protected Extensible Authentication Protocol (PEAP)*:** La autenticación PEAP permite la transmisión de otros EAP dentro del canal TLS.

Cuando se va a implementar autenticación 802.1x es recomendable utilizar el Servicio de Autenticación de Internet (IAS) de *Windows Server* 2003, como servidor RADIUS. Para realizar esta configuración es necesario permitir la autoinscripción al Servicio de Acceso Remoto (RAS) y a los certificados del servidor IAS, por lo que se debe verificar que la cuenta de computadora del servidor RADIUS pertenece a un grupo con permisos de lectura, inscripción y autoinscripción al RAS y al servidor IAS. Otras medidas que deben ser revisadas son:

1 Garantizar que el RAS y las plantillas de certificados del servidor IAS no requieren de la entrada de un usuario para autoinscripción.
2 Garantizar que el RAS y las plantillas de certificados del servidor IAS están disponibles en la autoridad de certificación (*Enterprise CA*).
3 Garantizar que la cuenta de computadora del servidor RADIUS esta disponible en la OU donde son aplicados, en las computadoras, los ajustes de autoinscripción definidos en el Grupo de Políticas.

En la figura 3.1 se muestra el proceso de autenticación 80.2.1x.

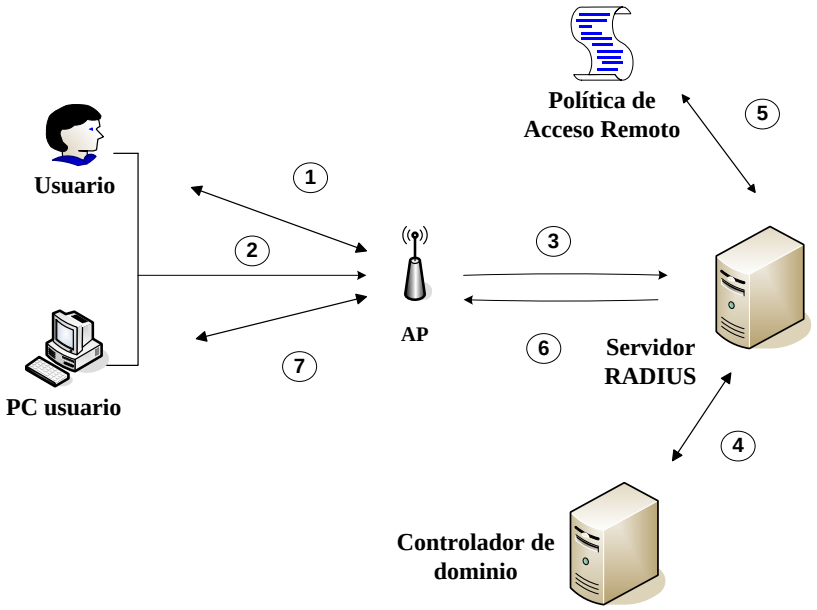

Figura 3.1 Proceso de autenticación 802.1x.

1. La computadora intenta asociarse con el WAP, el cual responde que el usuario debe proporcionar autenticación EAP.
2. LA computadora o el usuario pasan sus cartas credenciales a WAP:
   - Usando autenticación EAP\TLS, una petición firmada es presentada a WAP, prueba de que el usuario o la computadora tiene acceso a la llave privada asociada al certificado de autenticación de cliente.
   - Usando autenticación PEAP los usuarios deben introducir manualmente su cuenta de usuario y contraseña para el proceso de autenticación.
3. El WAP traduce paquetes de autenticación EAP en paquetes de autenticación RADIUS y los envía al servidor del mismo nombre.
4. El servidor RADIUS contacta con el controlador de dominio para validar la identidad del usuario.
5. El servidor RADIUS decide si un usuario o computadora tiene acceso a la red inalámbrica de acuerdo a la configuración de las políticas de acceso inalámbrico.
6. El servidor RADIUS envía al WAP un mensaje de éxito o fracaso del proceso de autenticación.
7. El WAP envía al usuario inalámbrico un mensaje EAP de éxito o fracaso del

intento de conexión.

La configuración actual de autenticación con la red inalámbrica es mediante WAP, un servidor RADIUS y los usuarios UCLV. El nivel de autenticación es bastante fuerte, utilizando las propias contraseñas de los usuarios, sin embargo, una PKI daría un nivel de fortaleza mayor a través de un proceso mucho más sencillo para el usuario.

3.8.1 Implementando autenticación 802.1x

Para implementar autenticación 802.1x es necesario configurar el servidor de RADIUS y WPA. En una red de *Microsoft*, para desplegar IAS como un servidor RADIUS de una red inalámbrica es necesario:

1. **Instalar IAS**: Para instalar IAS en un servidor de *Windows 2003* es necesario realizar esta operación como un usuario miembro del grupo de administradores. Desde el menú de inicio se accede a *Control Panel*\ *Add or Remove Programs*\ *Add/Remove Windows Components*\ *Networking Services*\ *Details* y en la nueva ventana se habilita *Internet Authentication Services*.
2. **Añadir el servidor IAS al RAS y al Grupo de Servidores IAS**: Una vez que es instalado el IAS se debe añadir la cuenta de la computadora del servidor IAS al RAS y al grupo de los servidores IAS del dominio. Para realizar esta operación se debe pertenecer al grupo de administradores del dominio. Luego desde *Administrative Tools*\ *Active Directory Users and Computers* se debe verificar que se esta trabajando en el mismo dominio donde esta ubicado la cuenta de computadora del servidor IAS. En el árbol de consola del *Active Directory Users and Computers* se expande el dominio y se accede a *Users*\ *RAS and IAS Servers group*\ *Members*\ *Add*. En la ventana de *Select Users, Contacts, Computers, or Groups* se selecciona *Object Types* y se asegura que la casilla de computadoras esta habilitada. En al selección de nombres de objeto se especifica el nombre de la computadora donde radica el IAS, dándose por terminada la configuración
3. **Definir los usuarios de RADIUS**: Cada WAP que emite peticiones de autenticación al servidor de RADIUS debe ser añadido a la lista de usuarios conocidos de WAP, debe ser dado a conocer su dirección IP y debe ser definida

una contraseña para RADIUS.

Para definir los usuarios de RADIUS se accede a *Administrative Tools*\ *Internet Authentication Service*\ *RADIUS Clients* (menú contextual)\ *New RADIUS Client.* En la ventana de *Name and Address* se define en el recuadro de *Friendly Name* un nombre con carácter descriptivo para WAP y en el recuadro de *Client Address* se especifica la dirección IP de WAP. En la información adicional se elige un vendedor de WAP, en caso de que el vendedor no se encuentre disponible, se habilita la opción estándar (RADIUS) y se introduce una contraseña para WAP. Este proceso debe repetirse para cada WAP que usa al servidor IAS para autenticación 802.1x (Komar and Team, 2008)

4. **Crear una política de acceso remoto para cuentas de computadoras**: Una vez que han sido definidos los usuarios del servidor RADIUS, es necesario crear una política de acceso remoto para cuentas de computadoras. Para realizar este proceso desde *Administrative Tools*\ *Internet Authentication Service* se despliega la opción de *Remote Access Policies*, eliminándose cualquier política de acceso remoto que aparezca por defecto. Luego en esta misma ventana se selecciona *New Remote Access Policy*\ *Use the Wizard to Set Up a Typical Policy for a Common Scenario*, especificándose que el nombre de la política es Computadoras Inalámbricas (*Wireless Computers*). En la ventana de *Access Method* se selecciona *Wireless*\ *Group*\ *Add*. En la selección de los grupos se elige *Domain**Domain Computers***.** Agregar grupos de cuentas de computadoras para que puedan conectarse a la red inalámbrica, es una operación que debe realizarse en cada dominio dentro del bosque. En la ventana de *Authentication Methods* se selecciona los métodos de autenticación, estos pueden ser mediante *smart cards* o otros certificados y se procede a configurar estos métodos (*Configure*). Para esta configuración en la ventana *de Smart Card or Other Certificate Properties* se elige *Certificate Issued to DNSName* (donde *DNSName* es el nombre asignado al DNS ó el de servidor IAS). Luego en *Completing the New Remote Access Policy Wizard* se finaliza la operación.

   Para completar el proceso de creación de políticas se accede a *Wireless*

Computers\ *Settings*\ *NAS-Port-Type*\ *Edit*. En el cuadro de *NAS-Port-Type* de la lista *Selected Types*, se selecciona *Wireless*, cualquier otra opción que aparezca seleccionada debe ser removida de la lista. Se continúa con *Settings*\ *Edit Profile*\ *Encryption*, borrándose en la pestaña de *Encryption* cualquier tipo de codificación, excepto *Strongest Encryption* (*MPPE 128 Bit*).

5. **Crear una política de acceso remoto para cuentas de usuarios**: Aunque el proceso de creación y configuración de políticas de acceso remoto para cuentas de usuario es similar al de las cuentas de computadoras, la diferencia principal radica en que la Organización de Usuario Inalámbrico requiere de un OID en el certificado de usuario.

   Para comenzar a crear la política de Acceso Remoto se accede a *Administrative Tools*\ *Internet Authentication Service*\ *Remote Access Policies*\ *New Remote Access Policy*\ *Use the Wizard to Set Up a Typical Policy for a Common Scenario* especificándose que el nombre de la política es Usuarios Inalámbricos (*Wireless Users*). En la ventana de *Access Method* se selecciona *Wireless*\ *Group*\ *Add*. En la selección de los grupos se elige *Domain**Domain Users*. En la ventana de *Authentication Methods* se selecciona los métodos de autenticación (*smart card* ó otros certificados) y se procede al configurarlos. En la ventana *de Smart Card or Other Certificate Properties* se elige *Certificate Issued to DNSName* (donde *DNSName* es el nombre asignado al DNS ó el de servidor IAS). Luego se accede a *Wireless Computers*\ *Settings*\ *NAS-Port-Type*\ *Edit* y de la lista *Selected Types* del recuadro de *NAS-Port-Type*, se selecciona Wireless; cualquier otra opción que aparezca seleccionada debe ser removida de la lista. Se continúa con *Settings*\ *Edit Profile*\ *Encryption*, borrándose en la pestaña de *Encryption* cualquier tipo de codificación, excepto *Strongest Encryption* (*MPPE 128 Bit*). En *Edit Dial-in Profile*\ *Advanced*\ *Add* se selecciona de la lista de atributos, *Allowed-Certificate-OID**Add**Add*. En la ventana de *Attribute Information* se selecciona como valor de atributo, *OID* (es el asignado a la organización en la aplicación de políticas para usuarios inalámbricos) y se finaliza el proceso.

3.8.2 Configuración de puntos de acceso inalámbricos

La configuración de WPA para puntos de acceso inalámbricos esta en dependencia del *Internetwork Operating System* (*IOS*) que se tenga instalado. Se debe garantizar que queden definidos los ajustes siguientes:

1. Configurar WAP para autenticación RADIUS.

o Anadir la dirección IP del servidor IAS para la autenticación RADIUS.

o Habilitar entrada secreta en RADIUS para el servidor IAS.

o Definir puerto de escucha en RADIUS para el servidor IAS (recomendado puerto de UDP 1812).

2. Configurar WAP para implementar la contabilidad de RADIUS.

o Anadir la dirección IP del servidor IAS para la contabilidad de RADIUS.

o Habilitar entrada secreta en RADIUS para el servidor IAS.

o Definir puerto de escucha en RADIUS para el servidor IAS (recomendado puerto de UDP 1813).

3.8.3 Configuración de la conexión a la red inalámbrica

Una vez que la infraestructura ha sido instalada correctamente los usuarios inalámbricos pueden conectarse la red utilizando autenticación 802.1x. Para iniciar la conexión en el *Network Connections de Windows* se accede a *wireless adapter* (menú contextual)\ *Properties*\ *Wireless Networks* (pestaña)*\ Preferred Networks* (sección)*\ Service Set Identifier (SSID)*\ *Properties*\ *Association* (pestaña) y se definen los siguientes ajustes:

Opción	WEP	WAP
Autenticación de Red.	Open	WPA or WPA-PSK
Codificación de datos.	WEP	TKIP ó AES
La Llave es proporcionada para mí automáticamente.	Habilitar	Habilitar

TABLA 3.2

Opción	WEP	WAP
Habilitar autenticación 802.1x para red.	Permitido.	Permitido.
Tipo de EAP.	*Smart Card* ó otros certificados	*Smart Card* ó otros certificados
Autentificar como computadora cuando la información en la misma esta disponible.	Habilitar si la computadora es parte del bosque de dominio.	Habilitar si la computadora es parte del bosque de dominio.

TABLA 3.3

Para finalizar el proceso, en *Smart Card* ó otros certificados, se configuran las siguientes opciones:

1 ***Use my smart card*:** habilitado si se utiliza un certificado archivado en una tarjeta inteligente.
2 ***Use a certificate on this computer*:** habilitado si se utiliza un certificado almacenado en la base de datos de certificados de usuarios.
3 ***Use simple certificate selection* (recomendado):** habilitado si se utiliza un certificado cuyo nombre coincide con el nombre de entrada al sistema del usuario.
4 ***Validate server certificate*:** Habilitar si se requiere autenticación mutua.
5 ***Use a different user name for the connection*:** habilitar esta opción solo si la computadora no es un miembro del bosque de dominio, permitiéndole al usuario elegir un certificado que no contiene su nombre de usuario corriente.

3.9 Descripción de las pruebas realizadas

En el Laboratorio de Redes de la Facultad de Ingeniería Eléctrica se llevaron a cabo las pruebas experimentales relacionadas con los niveles de implementación de una Infraestructura de Llave Pública.

Antes de iniciar con la implementación de la infraestructura, se creó un nuevo dominio dentro del laboratorio 224 (eli.uclv.edu.cu) y se instaló en las computadoras incluidas en la investigación el *software Internet Information Services* (IIS), indispensables en las pruebas que se fueron realizadas con páginas *web*. Los pasos seguidos par instalar IIS se encuentran descritos en el capitulo II, epígrafe 2.3.2.

Luego se procedió a la implementación de una jerarquía de autoridades certificadoras. En este caso se utilizo una jerarquía de un nivel (*Enterprise Root CA)* como la descrita en el capitulo II, epígrafe 2.3.3, la cual fue instalada en la misma computadora donde radicaba el controlador de dominio. Una vez instalada la CA se procedió a realizar pruebas de despliegues de certificados. Para realizar esta operación inicialmente fue necesario publicar en la CA las plantillas de los certificados (Cap. II, epígrafe 2.6.1) que se deseaban publicar, luego utilizando la inscripción manual de certificados (Cap. II, epígrafe 2.8.1) se realizó el despliegue de los mismos a diferentes usuarios y computadoras pertenecientes al dominio. Entre los métodos de inscripción manual que se utilizaron, se encuentran las Páginas de Inscripción *Web* y *Certificate Request Wizard*, herramienta que trabaja a través del MMC. Los resultados de las pruebas realizadas en esta primera etapa de implementación de la jerarquía fueron satisfactorias; se logro implementar la CA con sus funcionalidades básicas de despliegue de certificados a todos los usuarios, computadoras, y dispositivos dentro del dominio

En una segunda etapa de pruebas se brindaron soluciones de seguridad integradas a los principales servicios. La codificación SSL vinculada a la protección de los datos transferidos entre un sitio *web* y los usuarios del mismo, constituye la primera de estas soluciones (Cap. III, epígrafe 3.5). Para desplegar este servicio fue necesario publicar en la CA plantillas de certificados de autenticación tanto de servidores como de usuarios. Luego de autentificar un sitio *web* (www.eli.uclv.edu.cu) y configurarlo de forma tal que utilizara

codificación SSL, se pudo comprobar que mediante de las plantillas de seguridad para SSL un sitio *web* puede quedar configurado de 3 formas diferentes.

- Un usuario siempre tendrá acceso a la página *web*, independientemente de que posea un certificado de autenticación.
- Un usuario siempre tendrá acceso a la página *web*, pero en caso de poseer un certificado de autenticación el sitio *web* lo reconoce.
- Un usuario no tendrá acceso a la página *web* a menos que posea un certificado de autenticación de usuario.

La integración de una PKI con codificación SSL para la navegación *web* fue una prueba donde se obtuvieron resultados aceptables. Mediante el uso de *sniffers* se pudo verificar la codificación de los paquetes en el canal de comunicación y con las configuraciones para SSL se incrementó el control de acceso de usuarios a sitios *web*. Por otra parte la utilización de certificados digitales para autenticación tanto de servidores como de usuarios introdujo un nivel de seguridad más robusto, culminado en un servicio de navegación *web* mucho más seguro y confiable.

La autenticación de usuarios y computadoras en redes inalámbricas mediante el uso de certificados digitales, constituyó otra de las aplicaciones de una infraestructura de llave pública que fue probada en los ensayos a escala de laboratorio.

Para la implementación de la autenticación 802.1x se siguieron los pasos definidos en el Cap. III epígrafe 3.8.1, y el despliegue de certificados de autenticación tanto a usuarios como a computadoras se realizó antes de configurar los puntos de acceso inalámbricos (Cap. III. epígrafe 3.8.2) y las conexiones a la red inalámbrica (Cap. III, epígrafe 3.8.3).

En el momento de culminar este trabajo no se habían obtenido resultados satisfactorios en las pruebas realizadas para esta aplicación .Aunque se logro que un usuario presentara sus credenciales ante un servidor RADIUS a través de WAP, por problemas de configuración que no pudieron ser determinados y corregidos debido al tiempo disponible, el proceso de autenticación mediante certificados no concluyo exitosamente. Por esta razón fue imposible establecer conexión con la red inalámbrica a través de este método de autenticación.

CONCLUSIONES

A partir de la culminación del presente trabajo se arribaron a las siguientes conclusiones:

- La PKI como el conjunto de componentes y políticas necesarias para crear, gestionar y revocar certificados digitales ha alcanzado un alto grado de madurez, permitiéndole ser implementada en la Intranet de la UCLV como una infraestructura de seguridad vinculada a los principales servicios de la misma.
- La Intranet de la Universidad cuenta con con los medios, tecnología, equipamientos, servicios y personal calificado para implementar una PKI eficiente. En la actualidad mecanismos de seguridad basados en técnicas criptográficas (certificados, firma digital, etc.) no se encuentran presentes en la mayoría de los servicios de la misma. Los métodos de autenticación tanto de usuarios, computadoras y dispositivos en la red con las principales aplicaciones, presentan vulnerabilidades, que pueden ser aprovechadas por atacantes sin que, necesariamente posean estos, un alto poder de cómputo. Estas deficiencias pueden ser minimizadas con la implementación de una jerarquía de autoridades certificadoras.
- Las pruebas realizadas demostraron que los servicios de certificados de *Windows Server 2003* refuerzan y simplifican el proceso de autenticación entre los servicios y aplicaciones, proporcionando transparencia al usuario final.
- Los resultados alcanzados culminan con una propuesta de configuración de los niveles de seguridad de los servicios integrados a la PKI, los cuales incluyen correo electrónico, codificación SSL y redes inalámbricas

RECOMENDACIONES

- Ampliar la propuesta de manera que abarque un mayor número de servicios de la Intranet.
- Continuar con las pruebas experimentales a escala de laboratorio de la autenticación mediante certificados digitales para redes inalámbricas presentada en este trabajo, con el fin de perfeccionar este mecanismo de autenticación.
- Aumentar la cultura criptográfica tanto de usuarios como de administradores de red para que sean aprovechadas todas las ventajas de seguridad asociadas a la implementación una PKI.
- Impartir cursos a los usuarios finales del uso de los servicios criptográficos ofrecidos por la Infraestructura de Llave Pública.
- Integrar servicios brindados en plataformas de *software* libre a la PKI.
- Contemplar en futuras propuestas la migración hacia una PKI sobre *Windows Server 2008*.

REFERENCIAS BIBLIOGRÁFICAS

(2005) IN TILBORG, H. C. A. V. (Ed. *ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY*. Springer Science+Business Media, Inc.

(2006) Computer Science: Publication: A PKI Based Secure Audit Web Server.

(2007) Account Authority Digital Signature (20010615) Anne & Lynn Wheeler.

ABADI, M., BURROWS, M., KAUFMAN, C. & LAMPSON Authentication and Delegation with Smart cards.

AL-KHOURI, A. M. & BAL, J. (2007) Digital Identities and the Promise of the Technology Trio: PKI, Smart Cards, and Biometrics. *Journal of Computer Science*.

BERTOLÍN, G. A. & BERTOLÍN, J. A. (2004) Identificación y análisis en torno a PKI: infraestructura de clave pública y su relación con los certificados digitales y la firma electrónica avanzada. *Revista Española de Electrónica***,** 62-66.

CHANDRA, P., MESSIER, M. & VIEGA, J. (2003) Network Security with OpenSSL. O'Reilly.

CLEVELAND, N. L. (2001) Implementing Site-to-Site IPSec Between a Cisco Router and Linux FreeS/WAN.

CROSS, D. B. & BEN-MENAHEM, A. (2004) Key Archival and Management in Windows Server 2003.

CROSS, D. B. & KINDER, C. B. (2004) Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure.

CRUZ, R. G. (2005) Infraestructura de Clave Pública. *PKI y Software Libre.*

DIERKS, T. & RESCORLA, E. (2006) RFC 4346: The Transport Layer Security (TLS) Protocol Version 1.1. *Request for Comments.* IETF.

ESPINOZA, M. P., SÁNCHEZ, M. X. & QUIZHPE, M. P. (2008) Implementació de una Infraestructura de Clave Pública (PKI) en una rede de pruebas., UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA.

ETTL, R. (2003) Understanding and Configuring IPSec between Cisco Routers.

GOFFEE, N., KIM, S. H., SMITH, S., TAYLOR, P., ZHAO, M. & MARCHESINI, J. (2004a) Greenpass: Decentralized, PKI-based Authorization for Wireless LANs. *3rd Annual PKI Research and Development Workshop***,** 2003-2004.

GOFFEE, N. C., KIM, S. H., SMITH, S., TAYLOR, P., ZHAO, M. & MARCHESINI, J. (2004b) Greenpass: Decentralized, PKI-based Authorization for Wireless LANs.

GOOTS, N., IZOTOV, B., MOLDOVYAN, A. & MOLDOVYAN, N. (2003) Modern Cryptography: Protect Your Data with Fast Block Ciphers. A-LIST, LLC.

HAGSTRÖM, Å. (2006) Understanding Certificate Revocation.

HAMANN, E. M., HENN, H., SCHACK, T. & SELIGER, F. (2001) Securing e-business applications using smart cards. *IBM Systems Journal,* 40**,** 635-647.

HELLEN, I. (2004) Administrar una infraestructura de claves públicas de Windows Server 2003

HOUSLEY, R., POLK, W., FORD, W. & SOLO, D. (2002) RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. *Request For Comment.* IETF

JOHNER, H., FUJIWARA, S., YEUNG, A. S., STEPHANOU, A. & WHITMORE, J. (2001) Deploying a Public Key Infrastructure. Deploying a Public Key Infrastructure.

JUNG, S. W. & JUNG, S. (2006) Forward Secure Password-Enabled PKI with Instant Revocation. *Lecture Notes in Computer Science,* 4043**,** 54-67.

KAMBOURAKIS, G., KONTONI, D. P. N., ROUSKAS, A. & GRITZALIS, S. (2007) A PKI approach for deploying modern secure distributed e-learning and m-learning environments. *Computers & Education,* 48**,** 1-16.

KARATSIOLIS, V., LIPPERT, M. & WIESMAIER, A. (2004) Using LDAP Directories for Management of PKI Processes.

KINDER, C. B. & CROSS, D. B. (2004) Advanced Certificate Enrollment and Management. *Microsoft Corporation*.

KOMAR, B. & TEAM, M. P. (2004) Microsoft Windows Server 2003 PKI and Certificate Security. IN DELRE, M., BANKAITIS, D. & BECKELAAR, R. (Eds.). Microsoft Press.

KOMAR, B. & TEAM, M. P. (2008) Microsoft Windows Server 2008 PKI and Certificate Security. IN DELRE, M., BANKAITIS, D. & BECKELAAR, R. (Eds.). Microsoft Press.

KUZMOWYCZ, G. (2001) E-MAIL SECURITY WITH S/MIME.

LEE, Y., PARK, Y., KIM, H., HONG, S.-M. & YOON, H. (2006) Rogue Public Key Registration Attack and the Importance of 'Proof of Possession' in the PKI Environment. *IEICE Transactions on Information and Systems,* E89-D**,** 2452-2455.

LIOY, A., MARIAN, M., MOLTCHANOVA, N. & PALA, M. (2006) PKI past, present and future. *International Journal of Information Security*, 5**,** 18-29.

LODOS, J., Y, N. G. & RODRÍGUEZ, Y. (2003) Infraestructuras de claves públicas en redes corporativas. *Centro de Ingeniería Genética y Biotecnología (CIGB.*

LÓPEZ, M. J. L. (2008) Criptografía y Seguridad en Computadores.

LUCAS, M. W. (2006) *PGP & GPG: email for the practical paranoid,* San Francisco, No Starch Press, Inc.

NAKHJIRI, M. & NAKHJIRI., M. (2005) AAA and network security for mobile access : radius, diameter, EAP, PKI,

and IP mobility. IN INC, J. W. S. (Ed.

NASH, A., DUANE, W. & JOSEPH, C. (2001) *PKI: Implementing and Managing E-Security,* New York, McGraw-Hill Inc.

PIÑÓN, M. A. P. & CAMACHO, M. R. (2007) Implantación de Servicios de PKI en el Canal Web de Internet del Banco de España. *Datamation: la revista española de tecnología de la Información para empresa***,** 56-60.

RAINA, K. (2003) PKI Security Solutions for the Enterprise: Solving HIPAA, E-Paper Act, and Other Compliance Issues. IN LONG, C., TULTON, A. O. & SMITH, A. (Eds.). Robert Ipsen

RANKL, W. & EFFING, W. (2003) *Smart Card Handbook*, John Wiley & Sons Ltd.

ROJAS, R. T. (2004) Seguridad en Redes de Mediana y Pequeña Empresa. *Departamento de Telecomunicaciones y Electrónica.* Universidad Central "Marta Abreus" de Las Villas.

SANTESSON, S. (2005) RFC 4262: X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities. *Request for Comments.* IETF.

SATIZÁBAL, C., PÁEZ, R. & FORNÉ, J. (2007) WAP PKI and certification path validation. *International Journal of Internet Protocol Technology,* 2**,** 88-95.

SCHAAD, J. & MYERS, M. (2008) RFC 5274: Certificate Management Messages over CMS (CMC): Compliance Requirements. *Request For Comments.* IETF.

SLAGELL, A. J., BONILLA, R. & YURCIK, W. (2006) A Survey of PKI Components and Scalability Issues. *IEEE International Performance, Computing, and Communications Conference (IPCCC'06)***,** 10.

XENITELLIS, S. S. (2001) The Open–source PKI Book: A guide to PKIs and Open–source Implementations. 2.4.6 ed.

ZEILENGA, K. (2006) RFC 4523: Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates. *Request For Comments.* IETF.

GLOSARIO

ACRS *Automatic Certificate Request Settings*

AES *Advanced Encryption Standard*

AIA *Authority Information Access*

CA *Certification Authority*

CDP *CRL Distribution Point*

CMC *Certificate Management Messages over CMS*

CP *Certification Policy*

CPS *Certificate Practice Statement*

CRL *Certificate Revocation List*

DES *Data Encryption Standard*

DNS *Domain Name Server*

EAP *Extensible Authentication Protocol*

EFS *Encrypting File System*

EKU *Client Authentication Enhanced Key Usage*

FTP *File Transfer Protocol*

GPO *Group Policy Objet*

HTTP *Hypertext Transfer Protocol*

IAS *Internet Authentication Services*

IIS *Internet Information Server*

IOS *Internetwork Operating System*

LDAP *Lightweight Directory Access Protocol*

MAC *Message Authentication Code*

MMC *Microsoft Management Console*

NNTP *Network News Transfer Protocol*

OID *Object*

OU *Organizational Unit*

OWA *Outlook Web Access*

PEAP *Protected Extensible Authentication Protocol*

PGP *Pretty Good Privacy*

PKCS *Public Key Cryptography Standards*

PKI *Public Key Infrastructure*

POP 3 *Post Office Protocol*

RA *Registration Authority*

RADIUS *Remote Authentication Dial-In User Service*.

RAS *Remote Access Services*

RFC *Request for Comment*

S/MIME *Secure/Multipurpose Internet Mail Extensions*

SET *Secure Electronic Transaction*

SHA *Secure Hash Algorithm*

SMTP *Simple Mail Transfer Protocol*

SPKI *Simple Public Key Infrastructure*

SSL *Secure Socket Layer*

TCP *Transmission Control Protocol*

TKIP *Temporal Key Integrity Protocol*

TLS *Transport Layer Security*

UDP *User Datagram Protocol*

UNC *Universal Naming Convention*

UPN *User Principal Name*

URL *Uniform Resource Locator*

WEP *Wired Equivalent Privacy*

WPA *Wi-Fi Protected Access*

WTLS *Wireless Transport Layer Security*

ANEXOS

Anexo I Contenido del archivo *CAPolicy.inf* para CAs de distintos niveles de la jerarquía

Capolicy.inf **para la Autoridad Certificadora Raíz (1 nivel, *Enterprise Root CA*)**

```
[Version]
Signature="$Windows NT$"

[certsrv_server]
renewalkeylength=2048
RenewalValidityPeriodUnits=10
RenewalValidityPeriod=years
CRLPeriod=days
CRLPeriodUnits=2
CRLDeltaPeriodUnits=12
CRLDeltaPeriod=hours

[CRLDistributionPoint]
Empty=True

[AuthorityInformationAccess]
Empty=Trae
```

Capolicy.inf **para la Autoridad Certificadora Raíz (2 niveles, *Standalone Root CA*)**

```
[Version]
Signature="$Windows NT$"

[certsrv_server]
renewalkeylength=4096
RenewalValidityPeriodUnits=0x20
RenewalValidityPeriod=years
CRLPeriod=weeks
```

CRLPeriodUnits=26
CRLDeltaPeriodUnits=0
CRLDeltaPeriod=days

[CRLDistributionPoint]
Empty=True

[AuthorityInformationAccess]
Empty=True

Capolicy.inf para la Autoridad Certificadora Emisora (2 niveles, _Standalone Root CA_)

[Version]
Signature="$Windows NT$"

[PolicyStatementExtension]
Policies=Uclv CPS

[Uclv CPS]
OID=1.3.6.1.4.1.311.509.3.1
NOTICE= Universidad Central Marta Abreu de Las Villas
URL=http:// certpub.uclv.edu.cu /CPS/CPStatement.asp
renewalkeylength=2048
RenewalValidityPeriodUnits=5
RenewalValidityPeriod=years
CRLPeriod=3
CRLPeriodUnits=days
CRLOverlapPeriod=4
CRLOverlapUnits=hours
CRLDeltaPeriod=12
CRLDeltaPeriodUnits=hours
DiscreteSignatureAlgorithm=1
LoadDefaultTemplates=0

Capolicy.inf para la Autoridad Certificadora Raíz (3 niveles, _Standalone Root CA_)

[Version]
Signature="$Windows NT$"

[certsrv_server]
renewalkeylength=4096
RenewalValidityPeriodUnits=5
RenewalValidityPeriod=years

CRLPeriod=weeks
CRLPeriodUnits=26
CRLDeltaPeriodUnits=0
CRLDeltaPeriod=days

[CRLDistributionPoint]
Empty=True

[AuthorityInformationAccess]
Empty=True

***Capolicy.inf* para la Autoridad Certificadora de Políticas (3 niveles, *Policy CA*)**

[Version]
Signature="$Windows NT$"

[PolicyStatementExtension]
Policies=UCLV_POLICY1

[UCLV_ POLICY1]
OID=1.3.6.1.4.1.311.509.3.1
NOTICE=Universidad Central Marta Abreu de Las Villas
URL=http://certpub.uclv.edu.cu/CPS/CPStatement.pdf

[certsrv_server]

RenewalKeyLength=2048
RenewalValidityPeriodUnits=3
RenewalValidityPeriod=years

CRLPeriod=weeks
CRLPeriodUnits=6
CRLDeltaPeriodUnits=0
CRLDeltaPeriod=days

***Capolicy.inf* para la Autoridades Certificadoras Emisoras (3 niveles, *Issuing CA*)**

[Version]
Signature="$Windows NT$"

[certsrv_server]
renewalkeylength=2048
RenewalValidityPeriodUnits=3
RenewalValidityPeriod=years

CRLPeriod=3
CRLPeriodUnits=days
CRLDeltaPeriod=12
CRLDeltaPeriodUnits=hours

.

Anexo II *Scripts* de posinstalación para CAs de distintos niveles de la jerarquía

Script de postinstalación de la Autoridad Certificadora Raíz (1 nivel, _Enterprise Root CA_)

```
::Declare Configuration NC
certutil -setreg ca\DSConfigDN CN=Configuration, DC=uclv,DC=edu, DC=cu

 ::Define CRL Publication Intervals
certutil -setreg CA\CRLPeriodUnits 2
certutil -setreg CA\CRLPeriod “Days"
certutil -setreg CA\CRLDeltaPeriodUnits 12
certutil -setreg CA\CRLDeltaPeriod “Hours"
::Apply the default CDP Extension URLs
certutil -setreg CA\CRLPublicationURLs “65:%windir%\system32\CertSrv\
CertEnroll\%%3%%8%%9.crl\n79:ldap:///
CN=%%7%%8,CN=%%2,CN=CDP,CN=Public                                    Key
Services,CN=Services,%%6%%10\n6:http://%%1/
CertEnroll/%%3%%8%%9.crl\n0:file://\\%%1/CertEnroll\%%3%%8%%9.crl"

::Apply the default AIA Extension URLs
certutil -setreg CA\CACertPublicationURLs “1:%windir%\system32\CertSrv\
CertEnroll\%%1_%%3%%4.crt\n3:ldap:///
CN=%%7,CN=AIA,CN=Public                                              Key
Services,CN=Services,%%6%%11\n2:http://%%1/CertEnroll/
%%1_%%3%%4.crt\n0:file://\\%%1\CertEnroll\%%1_%%3%%4.crt"

::Enable all auditing events for the enterprise root CA
certutil -setreg CA\AuditFilter 127

 “Years"

::Restart Certificate Services
net stop certsvc & net start certsvc
sleep 5
```

certutil –crlg

Script de postinstalación de la Autoridad Certificadora Raíz (2 y 3 niveles, _Standalone Root CA_)

::Declare Configuration NC

certutil -setreg CA\DSConfigDN CN=Configuration,DC=uclv,DC=edu,DC=cu

::Define CRL Publication Intervals

certutil -setreg CA\CRLPeriodUnits 26

certutil -setreg CA\CRLPeriod “Weeks"

certutil -setreg CA\CRLDeltaPeriodUnits 0

certutil -setreg CA\CRLDeltaPeriod “Days"

::Apply the required CDP Extension URLs

Certutil -setreg CA\CRLPublicationURLs “65:%windir%\system32\CertSrv\CertEnroll\%%3%%8%%9.crl\n79:ldap:///CN=%%7%%8,CN=%%2,CN=CDP,CN=Public Key Services,CN=Services,%%6%%10\n6:http://certpub.uclv.edu.cu/CertData/%%3%%8%%9.crl"

::Apply the required AIA Extension URLs

Certutil -setreg CA\CACertPublicationURLs “1:%windir%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n3:ldap:///CN=%%7,CN=AIA,CN=Public Key Services,CN=Services,%%6%%11\n2:http://certpub.uclv.edu.cu/CertData/%%1_%%3%%4.crt"

::Enable all auditing events for the UCLV Root CA

certutil -setreg CA\AuditFilter 127

::Set Validity Period for Issued Certificates

certutil - setreg CA\ValidityPeriodUnits 10

certutil -setreg CA\ValidityPeriod “Years"

::Restart Certificate Services

net stop certsvc & net start certsvc

sleep 5

certutil –crl

::Copy the Root CA certificates and CRLs to the Floppy Drive

echo Insert a Floppy disk in Drive A:

sleep 5

copy /y %windir%\system32\certsrv\certenroll*.cr? a:\

***Script* de postinstalación de Autoridades Certificadoras de Políticas (*Policy CA*).**

::Declare Configuration NC

certutil - setreg CA\DSConfigDN CN=Configuration,DC=uclv,DC=edu,DC=cu

::Define CRL Publication Intervals

certutil -setreg CA\CRLPeriodUnits 26

certutil -setreg CA\CRLPeriod “Weeks"

certutil -setreg CA\CRLDeltaPeriodUnits 0

certutil -setreg CA\CRLDeltaPeriod “Days"

::Apply the required CDP Extension URLs

certutil- setreg CA\CRLPublicationURLs “65:%windir%\system32\CertSrv\CertEnroll\%%3%%8%%9.crl\n79:ldap:///CN=%%7%%8,CN=%%2,CN=CDP,CN=Public Key Services,CN=Services,%%6%%10\n6:http://certpub.uclv.edu.cu/CertData/%%3%%8%%9.crl"

::Apply the required AIA Extension URLs

certutil-setreg CA\CACertPublicationURLs “1:%windir%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n3:ldap:///CN=%%7,CN=AIA,CN=Public Key Services,CN=Services,%%6%%11\n2:http://certpub.uclv.edu.cu/CertData/%%1_%%3%%4.crt"

::Enable all auditing events for the UCLV Policy CA

certutil -setreg CA\AuditFilter 127

::Set Validity Period for Issued Certificates

certutil -setreg CA\ValidityPeriodUnits 5

certutil -setreg CA\ValidityPeriod “Years"

::Restart Certificate Services

net stop certsvc & net start certsvc

sleep 5

<u>*Script* de postinstalación de Autoridades Certificadoras Emisoras (*Issuing CA*).</u>

::Declare Configuration NC

certutil -setreg CA\DSConfigDN CN=Configuration,DC=uclv,DC=edu,DC=cu

::Define CRL Publication Intervals

certutil -setreg CA\CRLPeriodUnits 3

certutil -setreg CA\CRLPeriod “Days"

certutil -setreg CA\CRLDeltaPeriodUnits 12

certutil -setreg CA\CRLDeltaPeriod “Hours"

::Apply the required CDP Extension URLs

certutil-setreg CA\CRLPublicationURLs “65:%windir%\system32\CertSrv\CertEnroll\%%3%%8%%9.crl\n79:ldap:///CN=%%7%%8,CN=%%2,CN=CDP,CN=Public Key Services,CN=Services,%%6%%10\n6:http://certpub.uclv.edu.cu/CertData/%%3%%8%%9.crl\n6:http://%%1/CertEnroll/%%3%%8%%9.crl\n0:file://\\%%1/CertEnroll\%%3%%8%%9.crl"

::Apply the required AIA Extension URLs

certutil-setreg CA\CACertPublicationURLs “1:%windir%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n3:ldap:///CN=%%7,CN=AIA,CN=Public Key Services,CN=Services,%%6%%11\n2:http://www.fabrikam.com/CertData/%%1_%%3%%4.crt\n2:http://%%1/CertEnroll/%%1_%%3%%4.crt\n0:file://\\%%1\CertEnroll/%%1_%%3%%4.crt “

::Enable all auditing events for the UCLV mailsign

```
certutil -setreg CA\AuditFilter 127

::Set Maximum Validity Period for Issued Certificates
certutil -setreg CA\ValidityPeriodUnits 2
certutil -setreg CA\ValidityPeriod “Years"

::Restart Certificate Services
net stop certsvc & net start certsvc
sleep 5
certutil –crl

::Copy the issuing CA certificates and CRLs to the Floppy Drive
Echo Insert a Floppy disk in Drive A:
sleep 5
copy /y %windir%\system32\certsrv\certenroll\*.cr? a:\
```

Anexo III *Scripts* utilizados en E224 *Root CA*

Capolicy.inf

```
[Version]
Signature="$Windows NT$"
[certsrv_server]
renewalkeylength=2048
RenewalValidityPeriodUnits=10
RenewalValidityPeriod=years
CRLPeriod=days
CRLPeriodUnits=2
CRLDeltaPeriodUnits=12
CRLDeltaPeriod=hours
[CRLDistributionPoint]
Empty=True
[AuthorityInformationAccess]
Empty=True
```

***Script* de postinstalación**

```
::Declare Configuration NC
certutil -setreg ca\DSConfigDN CN=Configuration,DC=L224,DC=uclv,DC=edu,DC=cu
::Define CRL Publication Intervals
certutil -setreg CA\CRLPeriodUnits 2
certutil -setreg CA\CRLPeriod “Days"
certutil -setreg CA\CRLDeltaPeriodUnits 12
certutil -setreg CA\CRLDeltaPeriod “Hours"
::Apply the default CDP Extension URLs
certutil-setregCA\CRLPublicationURLs
“65:%windir%\system32\CertSrv\CertEnroll\%%3%%8%%9.crl\n0:file://\\%%1/CertEnrol
l\%%3%%8%%9.crl
::Apply the default AIA Extension URLs
certutil-setregCA\CACertPublicationURLs
“1:%windir%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n0:file://\\%%1\CertEnrol
l\%%1_%%3%%4.crt"
```

::Enable all auditing events for the enterprise root CA

certutil -setreg CA\AuditFilter 127

::Set Validity Period for Issued Certificates

certutil -setreg CA\ValidityPeriodUnits 2

certutil -setreg CA\ValidityPeriod "Years"

::Restart Certificate Services

net stop certsvc & net start certsvc

timeout /t 5

CertUtil –CRL

pause

***Script* de publicación de Plantillas de Certificados**

::Remove the default templates for a W2K3 CA.

certutil -SetCAtemplates -Administrator

certutil -SetCAtemplates -DirectoryEmailReplication

certutil -SetCAtemplates -DomainControllerAuthentication

certutil -SetCAtemplates -EFSRecovery

certutil -SetCAtemplates -EFS

certutil -SetCAtemplates -DomainController

certutil -SetCAtemplates -WebServer

certutil -SetCAtemplates -Machine

certutil -SetCAtemplates -User

certutil -SetCAtemplates –SubCA

:Publish the required certificate templates

certutil -SetCAtemplates +EFS

certutil -setCAtemplates +KeyRecoveryAgent

certutil -setCAtemplates +EFSRecovery

certutil -setCAtemplates +CAExchange

pause