Universidad de las Ciencias Informáticas

Facultad 1

"Propuesta de integración del Gestor de Documentos Administrativos eXcriba con una Infraestructura de Clave Pública"

Trabajo de Diploma para optar por el título de Ingeniero en Ciencias de la Informática.

Autores: Yanaivy Alejo Soto
Haniel Cáceres Navarro

Tutor: Msc.Adrian Cid Almaguer
Co-Tutor: Ing. Marcel Sánchez Góngora
Ing. Reinier Elejalde Chacón

La Habana, 8 de julio de 2011

Declaración de autoría

Declaramos ser autores de la presente tesis y reconocemos a la UCI los derechos patrimoniales de la misma, con carácter exclusivo.

Para que así conste firmo la presente a los ____ días del mes de _____ del año _____.

Yanaivy Alejo Soto	Haniel Cáceres Navarro

Tutor	Co-Tutor	Co-Tutor
Msc.Adrian Cid Almaguer	Ing. Marcel Sánchez Góngora	Ing. Reinier Elejalde Chacón

“Crezcan como buenos revolucionarios. Estudien mucho para poder dominar la técnica que permite dominar la naturaleza. Acuérdense que la Revolución es lo importante y que cada uno de nosotros, solo, no vale nada. Sobre todo, sean siempre capaces de sentir en lo más hondo cualquier injusticia cometida contra cualquiera en cualquier parte del mundo. Es la cualidad más linda de un revolucionario.”

Agradecimientos

Yanaivy Alejo Soto

Quisiera agradecer a tantas personas que me han ayudado durante los cinco años de la carrera, e incluso antes de entrar a la UCI, que resulta imposible mencionarlos uno por uno, a pesar de que se lo merecen.

Agradezco:

A mi mamá por estar siempre a mi lado a pesar de la distancia, por el apoyo incondicional, por el consejo oportuno, por el aliento y la esperanza que siempre me da, incluso en los momentos más difíciles, por ser fuente de mi inspiración y mis ganas de salir adelante. Si no fuese por ti no hubiese podido llegar a escribir estas líneas y razones sobran para expresar lo orgullosa que estoy de tenerte en mi vida.

A mi papá que aunque ya no se encuentre entre nosotros me dio el sostén necesario para mantener viva la llama de la fe y la esperanza para terminar mi carrera y convertirme en una profesional, por haberme dado una correcta educación y ser junto a mi mamá los autores intelectuales de este sueño realizado.

A mi hermanita por ser mi guía, mi faro, por ser cómplices de mis problemas y sufrir calladamente mis sufrimientos.

A mi niño querido: mi sobrinito, por llenarme de tanta alegría en esta vida.

A mis queridos abuelos que aunque ya no están junto a mi siguen siendo mis ángeles de la guarda, los cuales me enseñaron mucho de la vida y me demostraron que el tesoro más grande que una persona puede ostentar es una familia unida.

A mi maravillosa familia que me ha dado todo su amor y ha confiado siempre en mí.

A Bea, Clara y Heriberto por haberme acogido como parte de su bella familia y estar ahí en todos los momentos que más he necesitado ayuda.

A mis amigas Dairelys y Dairilys que desde la secundaria y hasta los días de hoy me han brindado su apoyo ilimitado.

A mi novio Dashiell por regalarme esos momentos maravillosos que he vivido a su lado y brindarme siempre su comprensión y cariño en los momentos más difíciles.

A todas mis amistades que he cultivado durante estos 5 años, especialmente a aquellos que desde primer año nunca nos hemos separado: Yenisleydis (Yeny), Madisleidy (Mady), Luis Enrique (Luiso), Oscar Luis (Osky), Sergio (Sergito) a todos ellos, todo el amor del mundo y mi eterno agradecimiento por ser los amigos incondicionales que son.

A mi compañero de tesis Haniel por su empeño y dedicación y por su inmensa paciencia conmigo.

A mis tutores y a Joelsy, por su apoyo, críticas y recomendaciones durante la realización de este trabajo.

A esta Revolución, y a esta Universidad hija de las ideas guiada por nuestro Comandante en Jefe.

En fin gracias a todos los que de una forma u otra contribuyeron a mi formación profesional así como al desarrollo de este trabajo.

A todos ustedes, gracias.

Haniel Cáceres Navarro

A mi mamita linda, por existir siempre, por darme fuerza, por confiar en mi, por enseñarme que a veces cuando el mundo se nos viene encima puede ser porque le vamos con demasiadas fuerzas al mundo

A mi papá, por confiar en mi y darme fuerzas para seguir adelante, por hacer de mi la persona que no se cansa de buscar siempre la perfección en los detalles y con la necesidad de estar aprendiendo en todo momento.

A mi abuela yeya, la viejita más linda del mundo, mi casquito, que hoy ve como yo, un sueño realizado.

A la Nana, mi hermanita del alma, por abrazarme cuando lo necesitaba, por ser mi complemento y estar ahí siempre que la necesité.

A mi abuela Nena, por su confianza sin límites.

A mi abuelo Isaías, que donde quiera que esté, sabe que hoy se gradúa el revolucionario al que enseñó a dar los primeros pasos.

A mis abuelos Victor, Chicho y Adelfa que se que hoy estarían orgullosos de mí.

A mi tía Laicy, mi otra mamá, hermana y amiga...

A mi primo Luisito, por ser mi hermano de siempre.

A Yamilé, por todo su cariño y apoyo.

A Evaldo, por devolverle la sonrisa a mi mamá.

A toda mi familia por su apoyo y confianza.

A Ale, ese pequeñito que arrebató sonrisas de mi rostro cuando pensaba que ya no tenía razones para sonreir, sin hacer falta que estuviera a mi lado.

A Yanaivy, mi compañera de tesis, por no perder nunca las esperanzas.

A Fidel (Fidale) y a Josué (el Joshua) por demostrarme que puede que sea un soñador pero que no soy el único.

A Yare, por ser mi amiga y demostrarme que siempre se puede seguir diciendo te quiero y robando sonrisas.

A Edito, Raydelmys, Raydel, Lissy, Gelsys, Rafa, Yanet, Karen amigos que marcaran para siempre mi vida en esta Universidad.

A mi gente del grupo, los antiguos y los nuevos, por ser parte de mis mejores días en esta Universidad.

A Lisi, por darme apoyo siempre que lo necesité y esas ayudas inmensas para amanecer cuando trabajaba la tesis.

A la FEU, por demostrarme que si se puede echar a mover el mundo si se tienen ganas.

A los profes Joelsys, Reinier, Marcel, incondicionales siempre.

A esas personitas que me dieron fuerzas para seguir diciendo te quiero, Yuky, Claudia, Elizabeth, Yinelys, Mailen, Arlen, Yare, Yixi.

A Frank, a Julio, a Rolando, a Juan Danilo, a Michel, a Leo, Dashiell por ayudarme cuando me hizo falta.

A Freddy, Reinier, el Lachy, Marcos, Leyva, el Rene y a todo ese piquete que considero mis hermanitos.

A esta gran Revolución que me lo ha dado todo.

A mis dos eternos guías Fidel y el Che, porque sin pretender imitarlos no hubiera llegado a ser lo que soy.

A esta Universidad, por darme la oportunidad de ser jóven y de disfrutar de esta etapa de la vida de manera tan especial.

A todos los que de una forma u otra han hecho de mi la persona que soy.

Dedicatoria

Yanaivy Alejo Soto

A mis viejitos lindos (Ofelia y Antonio) que aunque ya no se encuentren siempre han sido mis guías, a ellos que con su magia me enseñaron a ver la vida de la mejor forma, que me desmostraron ser las personas más maravillosas que he conocido, esos que enfrentaban el día a día de frente sin temor a nada, con esa fuerza y entereza que nunca dejaban de sorprenderme, por enseñarme a levantarme y aprender de mis errores, por inculcarme valores que siempre llevaré conmigo. A ustedes le dedico este trabajo por haber sido los mejores abuelos del mundo.

Haniel Cáceres Navarro

A mi mamá y a mi papá, dos personas especiales y únicas, quisiera tenerlos siempre.
A mi hermana y amiga, mi Nanita del alma.
A mi abuela yeya, mi casquito.

Resumen

En la actualidad es la información el activo informático más valioso de las empresas, llegando en ocasiones a contener la vida de la institución y alcanzando un valor incalculable. Tanto el software como el hardware pueden ser caros pero fáciles de reponer, no ocurriendo esto con la información. Es por ello que mantener la confidencialidad, integridad y autenticidad de los documentos una vez que se encuentren en la red, constituye una necesidad para velar por la seguridad de la información. El Gestor de Documentos Administrativos (GDA) eXcriba no cuenta con una herramienta capaz de velar por la autenticidad de los archivos que gestiona, siendo esta una debilidad en la seguridad, ya que no existe el mecanismo que permita verificar la autenticidad de un documento a partir de su firma digital.

Tomando la situación descrita como punto de partida se define como el objetivo de la presente investigación, crear un módulo que permita la verificación de la firma digital, integrando a su vez el GDA eXcriba con una Infraestructura de Clave Pública (PKI). Con el desarrollo de la presente investigación se logra que lo que en algún momento constituyera una debilidad del GDA eXcriba, actualmente es una fortaleza. Una vez que el GDA eXcriba cuente con una herramienta capaz de integrar su contenido con una PKI, y brinde la posibilidad de verificar la autenticidad de los documentos a partir de su firma digital, el sistema poseerá el elemento, hasta el momento ausente, capaz de velar por la seguridad de la información.

Palabras claves: firma digital, seguridad, Infraestructura de Clave Pública.

Índice General

Introducción

En la actualidad con el surgimiento de Internet y el vertiginoso avance de la tecnología, el volumen de datos que circula por la red de redes va creciendo aceleradamente, surgiendo así la necesidad de mantener un control sobre los mismos. La información circulante se ha convertido en el activo más valioso para el desarrollo de la sociedad, por lo cual gestionarla de manera eficiente implica en gran medida, catalogar, consultar, acceder e integrar información y documentación que, en la mayor parte de los casos se encuentra dispersa sobre soportes no informáticos.

Cuba no se encuentra aislada de este desarrollo, la necesidad de establecer programas de administración de documentos en los organismos y empresas estatales, se convierte en un elemento indispensable para el aumento de la eficiencia, la productividad y el cumplimiento de los objetivos que hoy se propone el sistema socialista, en el cual la planificación tiene un papel fundamental. Enmarcados en un esfuerzo coherente demandado por los profundos cambios económicos a los que se enfrenta la humanidad y por supuesto el país, es indispensable el uso efectivo de todos los recursos disponibles, incluyendo, por supuesto, la información y el manejo de la misma de manera eficiente.

El avance acelerado de las tecnologías hace cada día más grande la brecha digital entre los países desarrollados y los del tercer mundo. Aún siendo Cuba un país limitado económicamente, lucha por mantenerse al mismo nivel de las grandes potencias desarrolladoras de software. Uno de los motores que va impulsando adelante el proyecto de informatizar la sociedad cubana, es sin dudas la Universidad de las Ciencias Informáticas (UCI).

Nacida al calor de la Batalla de Ideas, como un sueño del líder indiscutible de la Revolución Cubana, Fidel Castro Ruz, la UCI surge teniendo como uno de sus principales objetivos formar al personal calificado capaz de informatizar la sociedad cubana desde cada uno de los rincones de la isla. Fidel la definiera en el momento de su creación como una *“universidad innovadora, de excelencia científica, académica y*

productiva, que forma de manera continua profesionales integrales, comprometidos con la Patria, soporte de la informatización del país y la competitividad internacional de la industria cubana del software"(Castro Ruz, Fidel, 2004).

La vinculación docencia-producción que hoy existe en la universidad, ha logrado aportar su granito de arena a la sociedad cubana. Hoy, la tarea encomendada por el Comandante en Jefe es más palpable, las soluciones informáticas a muchas de las problemáticas que tiene el país ya son una realidad y continúan desplegándose.

El proceso de almacenamiento y gestión de documentos de la forma convencional, ha empezado a quedar obsoleto. La necesidad de contar con información actualizada y puntual es la premisa que se está manejando en estos tiempos. Como fruto de la fusión de productos físicos y lógicos de información, así como el procesamiento de datos en un entorno de racionalización de recursos y métodos de trabajo, surgen las soluciones y servicios de gestión documental y como una particularidad de estos los gestores de documentos de manera automatizada. Su implantación permite desde el punto de vista económico una importante reducción de costos en recursos humanos y de instalaciones.

En el Centro de Informatización Universitaria (CENIA) de la UCI se desarrolló una primera versión del Gestor de Documentos Admnistrativos (GDA) eXcriba, el cual permite a sus usuarios realizar las mismas actividades que tradicionalmente ha realizado la gestión documental. Entre otras de las características presentes en en el GDA eXcriba podrían mencionarse las actividades administrativas y técnicas inclinadas a la planificación, manejo y organización de la documentación producida y recibida por las entidades, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación, todo esto de forma automatizada.

La Norma ISO-15489 define la gestión documental como el área de la gestión responsable del control eficiente y sistemático de la creación, recepción mantenimiento y uso o destrucción de documentos, incluyendo los procesos para capturar y conservar evidencia e información sobre actividades y transacciones de la organización.[1]

Aún cuando la gestión documental es una realidad en el mundo de la informática, otros peligros también se ciernen en la era digital. A la par que las tecnologías se han ido desarrollando hasta convertirse en elementos indispensables en campos como la salud, la educación, la cultura y la política; también los

ataques informáticos han ido en ascenso, convirtiéndose en uno de los principales riesgos que hoy tiene la información una vez que se trata con datos sensibles a este tipo de ataques. Se hace imprescindible entonces, el manejo de los términos concernientes a la seguridad informática.

Los bienes informáticos de una institución estan compuesto por los activos informáticos de tipo hardware, software y datos, siendo generalmente estos últimos los más preciados para las mismas. Tanto el hardware como el software pueden ser caros pero fáciles de reponer, en cambio, los datos o la información pueden contener la vida de la entidad alcanzando en ocasiones un valor incalculable, es por ello que la seguridad de la información debe tener como objetivo garantizar aspectos como:

- **Confidencialidad**: La información o los activos informáticos son accedidos solo por las personas autorizadas para hacerlo.
- **Integridad**: Los activos o la información solo pueden ser modificados por las personas autorizadas y de las formas previamente definidas.
- **Disponibilidad**: Los activos informáticos son accedidos por las personas autorizadas en el momento requerido.

Algunas fuentes como la revista RevistaLINUX.net entre otras aseguran que una de las soluciones más eficientes y completas en la actualidad cuando se habla de seguridad informática, son las infraestructuras de clave pública. Las cuales basan su funcionamiento en la criptografía de llave asimétrica para las operaciones criptográficas. Haciendo uso de un par de llaves, una pública conocida por todos y una privada solo conocida por el usuario a quien le es asignada.

Una vez que los datos se encuentren en la red es el uso de la firma digital quien garantiza la integridad de la información, mientras el cifrado es el encargado de velar por la confidencialidad de la misma, por otra parte el certificado digital es el encargado de velar por la autenticidad del emisor ante el receptor. Cada uno de ellos juega su papel cuando se trabaja en base a un sistema seguro.

La integración de sistemas independientes con infraestructuras de clave pública provee a los mismos de las herramientas necesarias para velar por la seguridad de la información. Para la versión del GDA eXcriba existente, desarrollado en la universidad no se implementó un elemento tan importante para la autenticidad, integridad y confidencialidad de la gestión de documentos como la integración con una PKI. Lo que hacía

que aún cuando el sistema pudiera gestionar eficazmente los documentos, estuviera propenso a ataques informáticos capaces de dañar la información que el mismo manejaba, constituyendo así una debilidad del mismo. Partiendo de la presente problemática se define como **problema científico**: ¿Cómo integrar el GDA eXcriba con una PKI para lograr la autenticidad, integridad y confidencialidad de la gestión de documentos?

Definiéndose como **objeto de estudio** de la investigación: La interoperabilidad de sistemas independientes con infraestructuras de clave pública, enmarcando como **campo de acción**: los mecanismos para la integración de un sistema web desarrollado en la plataforma J2EE con una PKI.

Se plantea como **idea a defender**: La integración del GDA eXcriba con una PKI logrará la autenticidad, confidencialidad e integridad en la gestión de documentos no presentes en su versión 1.0.

Tomando como punto de partida esta premisa la presente investigación define como **objetivo general** integrar el GDA eXcriba con una PKI que permita la autenticidad, integridad y confidencialidad en la gestión de documentos.

Para darle solución al mismo se definen los siguientes **objetivos específicos**:

1. Realizar un análisis bibliográfico de las infraestructuras de clave pública.
2. Realizar propuesta de las funcionalidades que debe cumplir el GDA eXcriba para su integración con una PKI.
3. Validar parte de la propuesta de integración con una PKI mediante el desarrollo de un módulo para el GDA eXcriba.
4. Validar propuesta de integración realizando pruebas de caja negra al módulo que se propone.

Para darle cumplimiento a los objetivos específicos se plantean las siguientes **tareas de la investigación**:

1. Análisis de las infraestructuras de clave pública y su uso en sistemas independientes.
2. Elaboración del marco teórico a partir del estado del arte del tema existente en la actualidad.
3. Análisis del proceso de integración del Gestor de Contenido Empresarial (ECM por sus siglas en inglés Enterprise Content Management) Alfresco con una PKI.

4. Selección de la tecnologías, frameworks y funcionalidades presentes en la plataforma J2EE para la integración de una aplicación desarrollada en la misma con una PKI.
5. Elección de la metodología, las herramientas de desarrollo y lenguajes a utilizar en la implementación del módulo de integración con una PKI para el GDA eXcriba.
6. Elaboración del análisis y diseño del módulo de integración con una PKI para el GDA eXcriba.
7. Implementación del módulo que forma parte de la propuesta para la integración con una PKI.
8. Ejecución de pruebas de aceptación para asegurar la calidad del módulo para la integración del GDA eXcriba con una PKI.

Para un mejor desarrollo de la investigación se usaron los siguientes **métodos científicos**:

- Del nivel teórico:
  - Método histórico: El cual permitió consultar bibliografía referente al tema de investigación, toda su trayectoria, evolución y comportamiento.
  - Método lógico: Condujo a estructurar la documentación investigada de una manera organizada y cronológica, para así tener un mejor entendimiento de la misma.
  - Método de la Modelación: Facilitó la creación de modelos, representando de manera gráfica parte del contenido de la presente investigación.
  - Método Sistémico: El mismo se puso en práctica para estudiar la integración de las tecnologías utilizadas, mediante la determinación de sus componentes, así como la relación entre ellos. Esta relación determina por un lado la estructura y la jerarquía de cada componente y por otra parte su dinámica, siendo también la expresión del comportamiento del sistema como totalidad en que un componente depende de otro u otros.
- Del nivel empírico
  - Método de la observación: Se puso en práctica, al concebir de forma consciente la planificación de la investigación, orientada hacia el logro del objetivo previamente determinado.

  - Método experimental: El experimento permitió estudiar el objeto, crear las condiciones para verificar la idea a defender.

- Existió un apoyo sobre los procesos de:

  - Análisis: Permitió la división mental de lo investigado, en relaciones y componentes para una mejor comprensión.
  - Síntesis: Posibilitó establecer mentalmente la unión entre las partes previamente analizadas, resaltando sus principales características, conceptos y relaciones.
  - Documental: Permitió consultar bibliografía en fuentes de carácter documental tales como libros, artículos y ensayos.

El presente trabajo de diploma está compuesto por un resumen, una introducción, tres capítulos, conclusiones, recomendaciones, así como las referencias bibliográficas, bibliografía y un glosario de términos, donde se da cumplimiento a los objetivos planteados en el trabajo, a continuación se describen los principales aspectos abordados en cada unos de los capítulos:

Capitulo 1: Fundamentación teórica, donde se expondrán los principales conceptos relacionados con el estado del arte de los sistemas de cifrado y clave pública. Breve descripción de los principales estándares de datos criptográficos.

Capitulo 2: Propuesta de solución, se realiza la fundamentación de la propuesta que se realiza, se describe el flujo de los procesos involucrados en la solución a modo de comprenderlos totalmente. Se plantea la elaboración del modelo de dominio, los requisitos funcionales y no funcionales del sistema, así como la solución propuesta para el sistema que se desea diseñar.

Capitulo 3: Módulo libPKI, en este, se exponen a través de un conjunto de artefactos la solución que se le dará al problema en cuestión, dentro de los cuales son fundamentales el diagrama de interacción (secuencia y/o colaboración) del caso de uso. Además, se define la implementación del sistema, así como las pruebas que se le aplicarán al mismo. La estructura en clases y componentes que garanticen la capacidad operacional del mismo y los resultados de las pruebas realizadas al sistema a lo largo del ciclo de vida del producto.

Capítulo 1

Capítulo 1: Fundamentación teórica

En el presente capítulo se precisan elementos teóricos que sustentan la investigación y el desarrollo del tema propuesto, a través del estudio y análisis de soluciones existentes. Se tratan las principales definiciones relacionadas con las PKI, así como los estándares para su elaboración. Se describen además las tecnologías actuales de desarrollo utilizadas para el análisis, diseño e implementación del sistema sobre las cuales se apoya la propuesta.

1.1. Criptografía

Según el diccionario de la Real Academia Española la palabra criptografía proviene del griego kryptos, que significa escondido, y graphos, que significa escritura, y la define como el arte de escribir con clave secreta o de un modo enigmático.[2]

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas u organizaciones) y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.

En la actualidad, la criptografía es el arte y la ciencia que provee los medios necesarios para comunicar información de forma segura ocultando su contenido. Dentro de todas las ramas de la criptografía, una de las que más ha revolucionado el panorama actual de las tecnologías de la información es la de la firma digital: tecnología que busca asociar al emisor de un mensaje con su contenido de forma que aquel no pueda posteriormente repudiarlo.

1.1.1. Necesidad de cifrado

El crecimiento de Internet ha traído enormes cambios en numerosos aspectos de la economía, la enseñanza, el arte, la política, entre otros campos. Sin embargo, paralelo al desarrollo de la funcionalidad y actividades de la red, también se ha generado un nuevo tipo de ataques y explotación de vulnerabilidades que deben ser tratados para facilitar la correcta evolución de los servicios disponibles. Destacando a continuación los ataques más comunes:

- Suplantación de identidad: Un intruso malintencionado puede hacerse pasar por una identidad diferente.
- Reactuación: Uno o varios mensajes legítimos son repetidos para producir un efecto no deseado e ilegítimo.
- Modificación de mensajes: Una parte de un mensaje legítimo es alterada por una entidad malintencionada, o bien los mensajes son retrasados o reordenados con la intención de reproducir un efecto no autorizado.[3]

Ante este tipo de ataques la vulnerabilidad de la información una vez en la red crece indefinidamente, convirtiéndola en peligro potencial cuando se trate de información sensible que pueda poner en riesgo la integridad de las empresas o usuarios finales. La empresa líder en soluciones escalables para redes de alto rendimiento, Certes Networks[4] y otras como Ovun[5], abogan por el uso del cifrado de las redes Ethernet como alternativa fiable para velar por la seguridad de la transmisión de datos y el uso creciente de las redes sociales. Muchas son las empresas que hoy dirigen sus principales esfuerzos a mantener la seguridad de la información, entre ellas podemos nombrar a at&t y TeKa, que lo han visto como una necesidad debido al incremento de los ataques en la red. Es por ello que en la actualidad el término de seguridad de la información comienza a ser más utilizado. Entre las principales formas de enfrentar este tipo de ataques y amenazas es necesario proveer a los sistemas de ciertas medidas de seguridad:

- Autenticación: Demostrar la identidad de una persona o aplicación, para garantizar de que con quien se mantiene la comunicación es realmente quien afirma ser.

- Integridad: Se debe proveer de mecanismos que permitan demostrar que la información no ha sido manipulada.
- No repudio: Asegurar que no se puede rebatir la propiedad de la información.
- Confidencialidad: Mantener privada la información, es decir, sólo aquellos a los que va dirigida la información tienen acceso a ella.

Todas estas medidas conllevan a un fin común: si se logra cifrar la información y protegerla con ciertas medidas de seguridad, se podrán preveer en gran escala los ataque y amenazas al sistema.

1.1.2. Tipos de cifrado

En el mundo de la criptografía moderna se pueden diferenciar dos claras vertientes, la criptografía simétrica y la criptografía asimétrica o de clave pública. El proceso básico de cifrado es el siguiente:

La entidad A cifra el mensaje M utilizando una clave de cifrado K1, resultando un mensaje codificado C. La entidad A envía entonces el mensaje C a la entidad destinatario B. Ésta decodificará el mensaje con la clave de descifrado K2. De esta forma la entidad A debe conocer la clave K1 y la entidad B debe conocer la clave K2. En la forma de estas dos claves radican las diferencias entre los dos tipos básicos de cifrado. Denominados cifrados simétricos y asimétricos, como se contempla a continuación. [6]

Cifrado simétrico

En el caso de cifrado simétrico la clave de cifrado que se usa es la misma para cifrar y descifrar. La clave debe ser conocida tanto por el emisor como el receptor del mensaje y ambos deben mantenerla en estricto secreto, ya que si se conoce peligraría el contenido del mensaje.

Tiene como ventaja que el algoritmo es extremadamente sencillo y rápido. Sin embargo este sistema no es el más seguro, pues depende íntegramente del secreto de la llave con que se cifrará y descifrará el mensaje en todo momento, si esta clave cae en las manos equivocadas ya la información dejaría de ser segura. [6]

Cifrado asimétrico

Los sistemas de cifrado asimétrico o sistemas de cifrado de clave pública, otorgan a cada entidad usuario un par de claves, una clave pública y otra clave privada. El hecho de utilizar dos claves, es para evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos.

Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en una clave. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

La clave pública se puede distribuir libremente a cualquier entidad con la que se quiere establecer comunicación, pero la clave privada debe permanecer conocida tan sólo para la entidad propietaria de dicha clave. Ambas claves están relacionadas matemáticamente entre sí pero conocer una clave pública no aporta conocimientos sobre la clave privada con la que dicha clave pública está vinculada. Lo que se cifra con una de las dos claves de un par se descifra únicamente con la otra clave no usada en el proceso de cifrado.

El hecho de que se utilice una clave distinta para cifrado y descifrado conlleva una gran ventaja respecto al cifrado simétrico: la distribución de claves es más sencilla y segura, ya que cada par de claves se distribuye únicamente a su entidad propietaria. Para la comunicación entre dos entidades poseedoras de pares de claves basta con que intercambien sus claves públicas, acción que no supone ningún riesgo ya que no hace visible la clave privada. Sin embargo el sistema de cifrado asimétrico tiene varias desventajas respecto al cifrado simétrico:

- Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
- Las claves deben ser de mayor tamaño que las simétricas.
- El mensaje cifrado ocupa más espacio que el original.

A pesar de estas desventajas el cifrado asimétrico o de clave pública cubre varios de los aspectos mencionados con anterioridad: es capaz de aportar confidencialidad mediante el cifrado con la clave pública y de conseguir con algoritmos de firma digital el no repudio y la autenticación del remitente.

Un problema importante que se plantea en la criptografía de clave pública es la distribución de claves públicas, de forma que quede demostrado que una clave pública es auténtica y que no ha sido manipulada o sustituida por terceros maliciosos. La manera típica de resolver este problema es mediante el uso de una PKI. [6]

1.1.3. Aplicaciones directas: autentificación y firmas

Debido a la asimetría inherente al proceso de comunicación en los sistemas basados en el cifrado con clave pública, el uso de ambas claves es necesario, pero la clave privada debe permanecer secreta en manos del propietario. Teniendo esto como premisa este tipo de criptografía puede tener varios usos. En cada uno de ellos se alternan las funciones que cumplen la clave privada y la clave pública, como se muestra a continuación.

Un primer uso consiste en comprobar que dado un mensaje enviado por el emisor A, pueda comprobarse que dicho mensaje ha sido enviado solo por el emisor A. Lo que ocurriría de la siguiente forma: la entidad poseedora de un par de claves puede cifrar datos con su clave privada y enviarlos a otra entidad conocedora de la clave pública de la primera. En este caso, la entidad que recibe el mensaje cifrado puede descifrarlo y confirmar que dicho mensaje proviene de quien dice enviarlo, ya que si ha conseguido descifrar el mensaje con éxito, significa que ha sido cifrado con la correspondiente clave privada, lo que por lo tanto identifica al emisor. Para esto se necesita por supuesto que el formato del mensaje sea reconocible o que la entidad receptora sepa identificar cuándo un mensaje descifrado tiene sentido. El proceso descrito anteriormente es el usado en las firmas digitales.[7]

Otro uso de este tipo de cifrado es el contrario, asegurar que el único destinatario que pueda recibir un mensaje sea un destinatario B previamente conocido, este es el proceso conocido como auntentficación. Para esto es necesario que el emisor del mensaje A cifre el mensaje con la clave pública de B de manera que solo B pueda descifrar el mensaje usando su propia llave privada que debe ser secreta en todo momento. De esta forma sólo el auténtico poseedor de la clave privada de B podrá responder correctamente a un reto lanzado por la entidad A ante la que se quiere autenticar.

Firma digital

El proceso de firmado digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido, generando una huella digital del mensaje. Esta huella digital se encripta con la clave privada del firmante, y el resultado de esta operación es lo que se denomina firma digital la cual se enviará adjunta al mensaje original. El software de firma digital puede además efectuar varias validaciones, entre las cuales se encuentran:

- Vigencia del certificado digital del firmante. El certificado digital es un documento digital mediante el cual un tercero de confianza, generalmente utilizada la Autoridad Certificadora (CA), garantice la vinculación entre la identidad de un sujeto o entidad y su clave pública.
- Revocación del certificado digital del firmante (puede ser por Online Certificate Status Protocol (OCSP) o Certificate Revocation List (CRL)
- Inclusión de sellado de tiempo (mecanismo online que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo).[8]

El método o función hash es un algoritmo matemático, que permite calcular un valor resumen de los datos a ser firmados digitalmente. Funciona en una sola dirección, ya que no es posible calcular los datos originales a partir del resumen.

Para que sea de utilidad, la función hash debe satisfacer dos importantes requisitos. Primero, debe ser difícil encontrar dos documentos cuyo valor para la función "hash"sea idéntico. Segundo, dado uno de estos valores, debería ser difícil recuperar el documento que lo produjo.

Existen funciones hash específicamente diseñadas para satisfacer estas dos importantes propiedades. SHA y MD5 son dos ejemplos de este tipo de algoritmos.

Una vez el mensaje llega al receptor si el hash calculado en ese momento no coincide con el de la firma del emisor una vez decodificada entonces o bien el documento fue modificado tras la firma o la firma no fue generada con la clave privada del supuesto emisor. Este algoritmo provee al receptor de una fuerte herramienta para probar la autenticidad del documento.

Existen normas que definen los formatos técnicos de las firmas electrónicas como son las normas TS 101 733 y TS 101 903.

Siguiendo estas normas se definen varias modalidades de firma:

- Firma básica: Incluye el resultado de operación de hash firmado con la clave privada del firmante, el certificado asociado a la clave privada del firmante e identifica los algoritmos utilizados en el proceso de firma.
- Firma fechada: A la firma básica se añade un sello de tiempo calculado a partir del hash del documento y firmado por una TSA (Time Stamping Authority, autoridad de sellado de tiempo en español).
- Firma validada o firma completa: A la firma fechada se añade información sobre la validez del certificado procedente de una consulta de CRL o de OCSP realizada a la CA.
    - La firma completa libera al receptor del problema de ubicar al prestador de servicios de certificación responsable de gestionar las consultas de validez del certificado del firmante, y de determinar los procedimientos de validación disponibles.

Incorporando cualquiera de estas variantes de firmas al documento el firmante va a estar adjuntando al documento una marca que es única para ese documento y que sólo él es capaz de producir.

El receptor del mensaje podrá comprobar que el mensaje no fue modificado desde su creación y que el firmante es quien dice ser a través del siguiente procedimiento: en primer término el receptor generará la huella digital del mensaje recibido y luego descifrará la firma digital del mismo utilizando la clave pública del firmante obteniendo de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que el mensaje no fue alterado luego de creado y que el firmante es quien dice ser.[9]

1.2. Infraestructura de Clave Pública

En la actualidad cuando hablamos de criptografía, una PKI es una combinación tanto de hardware, software, personas, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas. Dichas operaciones pueden ser el cifrado, la firma digital o el no repudio de transacciones electrónicas entre otras.[10]

Una PKI establece una relación entre claves públicas y sus respectivas identidades de usuario por medio de una CA. La identidad de usuario debe ser única para cada CA. Este vínculo usuario-claves se establece a

través de un proceso de registro y expedición, que, dependiendo del nivel de garantías que posea el vínculo, será realizado mediante software en una Autoridad de Registro (RA) o bajo supervisión humana, esta ultima con mayor certeza de seguridad.

La PKI provee a los usuarios de vías que le permitan autenticarse frente a otros usuarios y usar la información de los certificados de identidad de estos (por ejemplo, las claves públicas) para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío, y otros usos. [11]

En una operación criptográfica que use PKI, intervienen conceptualmente como mínimo las siguientes partes:

- Un usuario que inicia la operación
- Una serie de autoridades, que den fe de la ocurrencia de la operación y garanticen la validez de los certificados implicados en la misma (CA, RA y TSA).
- Un destinatario de los datos cifrados/firmados/enviados, garantizados por parte del usuario que inició la operación (puede ser él mismo).

Durante las operaciones criptográficas de clave pública se realizan procesos o procedimientos en los que se utilizan algoritmos de cifrado conocidos y accesibles para todos. Por este motivo la seguridad que puede aportar la tecnología PKI, está fuertemente ligada a la privacidad de la llamada clave privada y los procedimientos operacionales o políticas de seguridad que se aplican a la misma, mientras más resguardada sea la llave privada, tanto más segura será la PKI.

Es de destacar la importancia de las políticas de seguridad que se implanten en este tipo de tecnología, puesto que ni los dispositivos más seguros ni los algoritmos de cifrado más fuertes sirven de nada si, por ejemplo, una copia de la clave privada protegida por una tarjeta inteligente criptográfica se guarda en un disco duro convencional de un PC conectado a Internet.[12]

1.2.1. Componentes de la Infraestructura de Clave Pública

En este apartado se definen los componentes más habituales de los que consta una PKI, así como ventajas y desventajas de la misma.

Usuario Subscriptor

El usuario suscriptor de una PKI es aquel que posee al menos un par de claves (pública y privada) junto con un certificado asociado a su clave pública y utiliza un conjunto de aplicaciones que hacen uso de la tecnología PKI para validar firmas digitales. Es el usuario que confía y hace uso de los certificados de los que es titular.[13]

Autoridad de Certificación (CA)

En criptografía una autoridad de certificación, certificadora o certificante es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública. Jurídicamente es un caso particular de Prestador de Servicios de Certificación.[8]

La CA, por sí misma o mediante la intervención de una RA, verifica la identidad del solicitante de un certificado antes de su expedición o, en caso de certificados expedidos con la condición de revocados, elimina la revocación de los certificados al comprobar dicha identidad. Los certificados son documentos que recogen ciertos datos de su titular y su clave pública y están firmados electrónicamente por la CA utilizando su clave privada. La CA es un tipo particular de Prestador de Servicios de Certificación que legitima ante los terceros que confían en sus certificados la relación entre la identidad de un usuario y su clave pública. La confianza de los usuarios en la CA es importante para el funcionamiento del servicio y justifica la filosofía de su empleo, pero no existe un procedimiento normalizado para demostrar que una CA merece dicha confianza.[8]

Una CA es una entidad o servicio que emite certificados. El sistema de CA es la base de confianza de una PKI, ya que gestiona los certificados de clave pública durante toda su vida. Cada certificado emitido por una CA debe estar firmado por una CA de mayor grado en el esquema jerárquico de autoridades certificadoras, formándose así una cadena de certificados, en los que unas CA se avalan a otras hasta llegar a la CA superior, que se avala a sí misma. La jerarquía de firmas y la cadena con ella formada están contempladas en el estándar X.509 v3, que indica la forma correcta de realizar estas cadenas de certificaciones.

Características de la CA:

- Emite certificados vinculando la identidad de un usuario o sistema a una clave pública con una firma digital
- Programa las fechas en la que expiran los certificados
- Garantiza que los certificados se revocan cuando sea necesario.

Autoridad de Registro (RA)

La RA es la responsable de verificar el vínculo entre los certificados (concretamente, entre la clave pública del certificado) y la identidad de sus titulares. Esta permite la descentralización agilizando así el proceso de certificación y aumentando la eficacia en la gestión de solicitudes.

Una RA proporciona el interfaz entre el usuario y el CA. Captura y autentifica la identidad de los usuarios y entrega la solicitud de certificado al CA. La calidad de este proceso de autentificación establece el nivel de confianza que puede otorgarse a los certificados. Es una parte opcional de la PKI que mantiene las identidades de aquellos usuarios de los que las autoridades de certificación pueden expedir certificados digitales. La RA es la entidad autorizada por la CA para proveer administración de tiempos de validez de los certificados.[14]

Repositorio

Los repositorios: son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de CRL. En una CRL se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecida dentro del mismo certificado[15].

Autoridad de Validación (VA)

La autoridad de validación (o, en inglés, VA, Validation Authority) es la encargada de comprobar la validez de los certificados digitales. Siendo además el componente que tiene como tarea suministrar información sobre la vigencia de los certificados electrónicos que, a su vez, hayan sido registrados por una RA y certificados por la CA.[16]

Autoridad de Sellado de Tiempo (TSA)

La TSA es la autoridad encargada de firmar los documentos con la finalidad de probar que existían y que no han sido alterados, antes de un instante de tiempo determinado. [17]

Un sellado de tiempo de confianza debe ser expedido por un tercero de confianza que actúa como TSA, de acuerdo con el estándar RFC 3161. Se utiliza para probar la existencia de ciertos datos antes de un determinado momento(por ejemplo contratos, datos de investigación, expedientes médicos) sin la alternativa de que el propietario pueda adelantar los sellos de tiempo. Múltiples autoridades de sellado de tiempo pueden ser usadas para aumentar la confianza y reducir la vulnerabilidad.

El nuevo estándar para sellados de tiempo de confianza ANSI ASC X9.95 Standard extiende el estándar RFC 3161 con requisitos de seguridad a nivel de datos para proveer integridad de los mismos a través de una fuente de tiempo de confianza y que sea probable para cualquier tercero.

La técnica de sellado de tiempo se basa en funciones de hash y firmas digitales. En primer lugar se calcula el hash de los datos a sellar. Este hash es enviado a la autoridad de sellado de tiempo, TSA, que concatena un sellado de tiempo al hash y calcula el hash de la concatenación resultante. Este segundo hash con la clave privada de la TSA es firmado digitalmente. El conjunto sellado de tiempo hash firmado se envía al solicitante del sellado de tiempo, que lo almacena junto con los datos originales. Esta técnica para el solicitante del sellado de tiempo es confidencial, dado que la TSA nunca va a llegar a ver los datos originales, tan sólo su hash, a partir del cual no se pueden obtener los datos que lo generan. [18]

Autoridad de Aprobación de Políticas (PAA)

La autoridad de aprobación de políticas PAA, por las siglas de Policy Approval Authority es una entidad a la que, sujeto a criterios de cada PKI, algunos usuarios de la infraestructura creada pueden ser invitados a formar parte de la misma.

Esta autoridad debe ejercer su rol de entidad neutral y representativa pero de vital importancia pues será la encargada de definir las políticas que se aplicarán a la misma infraestructura a la que pertenece. Por tanto, la composición y las reglas de la PAA son esenciales para garantizar la neutralidad y fiabilidad de toda la infraestructura. Se podrá buscar también participación de terceras partes que no sean necesariamente usuarios directos de la PKI como medio para asegurar más si cabe la neutralidad y confianza de dicha

estructura.[19]

Estas terceras partes pueden ser organizaciones internacionales, organizaciones no gubernamentales, gobiernos, compañías tecnológicas entre otros que puedan brindar su servicio con el fin de asegurar la neutralidad de las mismas.

La PAA debe emprender una labor constante de establecimiento y mantenimiento de políticas y prácticas que se apliquen a la PKI, supervisando de manera constante el desenvolvimiento y desarrollos tecnológicos, legales, políticos, culturales o económicos que afecten o puedan afectar la integridad de la infraestructura, intentando perseguir de la mejor manera posible los objetivos iniciales de la PKI.

1.2.2. Certificados digitales

Un certificado digital es un documento digital mediante el cual un tercero confiable una CA garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Es la certificación electrónica que emiten las CA donde constan unos datos de verificación de firma a un signatario y confirma su identidad. Entre los datos figuran la fecha de emisión y la fecha de caducidad, la clave pública y la firma digital del emisor.[20]

El certificado digital se convierte en el centro de la PKI pues es la confianza en terceros lo que provee a la misma de la seguridad a los usuarios. Con este fin los certificados digitales serían la principal herramienta a utilizar.

Si bien existen variados formatos para certificados digitales, los más empleados siguen el estándar ITUT-X.509.[21] Usando este estándar el certificado digital una vez creado contiene el nombre de la entidad certificada, número de serie, fecha de expiración, una copia de la clave pública del titular del certificado (utilizada para la verificación de su firma digital) y la firma digital de la autoridad emisora del certificado, de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación.

Un certificado digital puede ser generado por cualquier individuo o institución, pero si éste emisor no es reconocido por quienes interactúen con el propietario del certificado, el valor del mismo es prácticamente nulo. Por esta razón, los emisores deben acreditarse. Así se denomina al proceso por el cuál entidades reconocidas, generalmente públicas, otorgan validez a la institución certificadora, de forma que su firma pueda ser reconocida como fiable, transmitiendo esa fiabilidad a los certificados emitidos por la misma.

Estándar X.509

En el ámbito de la criptografía, el estándar X.509 es un estándar de la UIT-T (Sector de Normalización de de las Telecomunicaciones) en PKI para Single Sign On (SSO) y para infraestructuras de administración de privilegios. El estándar X.509 especifica, entre otras cosas, los formatos estándar para certificados de clave pública, listas de revocación de certificados, certificados de atributos y un algoritmo de validación de árboles de certificación.

Este estándar X.509 es revelado al público en julio de 1988, en sus inicios surge asociado con el estándar X.500. Asume un sistema estrictamente jerárquico de autoridades de certificación para expedir certificados. Este enfoque contrasta con otros modelos de webs de confianza, como PGP (Pretty Good Privacy), en los que cualquiera, no sólo autoridades de certificación especiales, pueden firmar y de esa forma atestiguar la validez de certificados de claves de otros.[21, 22]

Ya en su tercera versión el estándar X.509 incluye la flexibilidad de admitir otras topologías como puentes y mallas en los árboles de certificación, de forma que se adapta mejor a la organización cada vez más flexible de Internet.

En un sistema basado en el estándar X.509, una CA emite un certificado que vincula una clave pública a un nombre distintivo (Distinguished Name), según un enfoque X.500 tradicional en el que se basa el estándar X.509, o a un nombre alternativo (Alternative Name).

El Distinguished Name DN es un nombre globalmente único dentro de una PKI que cualquiera podría usar para referirse a la entidad a la que pertenece. El estándar X.509 mantiene la definición del estándar X.500 para este campo. En cambio el Alternative Name es novedad respecto al estándar X.500 ya que este añade flexibilidad al vincular una clave pública a un nombre, ya que permite asociarlo a una dirección de correo electrónico o una entrada de servidor de nombres de dominio DNS.

Existen navegadores como Internet Explorer, Mozilla, Opera, Safari, tienen certificados raíz preinstalados. De esta forma determinados certificados para comunicaciones sobre SSL, de grandes proveedores que han pagado por este privilegio, funcionarán de forma instantánea.

El estándar X.509 incluye también algunos métodos para implementar CRL aun cuando el método aprobado por la IETF de comprobar la validez de certificados es mediante el protocolo de estado de certificado en línea, OCSP por sus siglas en inglés.

1.2.3. Estado de las infraestructuras de clave pública a nivel internacional

En la actualidad existen un poco más de 20 países en el mundo con un marco legal establecido por sus respectivos gobiernos en el desarrollo de tecnologías de infraestructuras de clave pública. Conociendo este dato es posible darse cuenta que la utilización de las infraestructuras de clave pública se encuentra en un incipiente desarrollo y dando sus primeros pasos, aunque es válido tener en cuenta que no fue hasta 1997 que el RSA[1] salió a la luz pública.

La situación en Europa es muy distinta a lo que ocurre en la actualidad en Estados Unidos que son en su conjunto los principales exponentes de esta variante de la seguridad informática. En Estados Unidos reina una mayor libertad de mercado, pues las reglas no siempre son claras. Todo lo contrario ocurre en Europa donde la directiva de firma electrónica y las correspondientes leyes nacionales sobre la materia han restringido mucho el ámbito en el que se pueden mover los prestadores de servicios de certificación y los proveedores de este tipo de tecnologías. Esto podría afirmarse de la siguiente manera, en Europa son los gobiernos quienes deciden qué dispositivos de certificación son seguros y quién puede convertirse en prestador de servicios de certificación.[23] Además, en los países de la Unión Europea suele haber una autoridad auspiciada por el gobierno con vocación de establecerse como prestador de servicios genérico para facilitar el acceso a la firma electrónica por parte de las empresas o ciudadanos.

Por lo tanto la situación de las administraciones públicas no tienen nada que ver con el entorno privado, lo que ha traído consigo que estas últimas se han desarrollado de forma mucho más rápida, espoleadas por el boom de las empresas punto com y por la rápida implantación de productos de distribución de claves y comunicaciones seguras en las grandes empresas (como los bancos por ejemplo). Aunque esta implantación no se produjo de cara al cliente final, ha tenido un gran auge en los últimos tiempos.

Las empresas fabricantes de tecnologías de infraestructuras de clave pública que se crearon confiando en el boom de final del siglo pasado han sufrido un duro golpe debido a varios factores entre los que se encuentran el famoso 11 de septiembre o la ralentización de la adopción masiva del comercio electrónico. Sólo aquellos que se han diversificado en otros campos son las que se han mantenido y confían en el futuro prometedor y seguro que asegura el uso de las infraestructuras de clave pública.

[1] Sistema criptográfico de clave pública, las siglas provienen de sus 3 principales desarrolladores y propietarios de la empresa: Rivest, Shamir y Adleman

1.2.4. Estado de las infraestructuras de clave pública a nivel nacional

En Cuba el uso de las infraestructuras de clave pública también se encuentra en incipiente desarrollo. En el afán por seguir marcando pauta en el desarrollo de la informática y las comunicaciones nuestro país a realizado sus primeras investigaciones en el uso de las infraestructuras de clave pública.

De esta forma en el Ministerio del Interior ha desarrollado una PKI, a la cual se le han implementado varios procesos como son la validación y autenticación de certificados digitales.

En algunas universidades del país también se han realizado trabajos de diploma vinculados directamente al uso de estas infraestructuras, los cuales generalmente han estado asociados a las principales industrias de nuestro país, podemos citar por ejemplo el caso del Instituto Superior Politécnico José Antonio Echeverría, la Universidad Central de las Villas Marta Abreu y la UCI, todas en vías de profundizar en su uso.

Es precisamente en la UCI en la cual el uso de la PKI alcanza un poco más de profundidad permitiendo realizar firmas digitales para la validación de documentos así como validación y autorización de certificados digitales, elementos que han permitido garantizar la confiabilidad e integridad de documentos tales como las evaluaciones estudiantiles. El uso de esta última PKI ha sido la principal fuente de retroalimentación del presente trabajo.

1.2.5. Estado de la integración de Alfresco con infraestructuras de clave pública

En la actualidad Alfresco no cuenta con herramientas nativas para el uso de la firma digital siendo una parte vital del ciclo de vida de la gestión documental cuando se manejan documentos de alta sensibilidad. Es por ello que tanto la comunidad de desarrollo de Alfresco y otras empresas como INNOVASOFT New TecnoLogic se dedican al desarrollo de herramientas capaces de permitir el trabajo con la firma digital desde Alfresco.

Entre las iniciativas más destacadas cabe mencionar la tomada por la empresa INNOVASOFT New TecnoLogic y la vinculación de Alfresco con Sinadura Desktop.

INNOVASOFT New TecnoLogic desarrolló una herramienta capaz de asociar la firma digital con los documentos manejados por Alfresco, este módulo destaca entre sus principales características.

- Soporte para multi-firma (en serie y paralelo).

- Utilización de algoritmo criptográfico AES (sustituto de DES)
- Soporte para DNI electrónico, certificados de persona física de la FNMT, certificados de persona física de Camerfirma, etc ..
- Implementación de procesos de firma mediante workflows avanzados.
- Custodia segura de firmas.
- Validación de documentos firmados.

Aún cuando esta solución es capaz de resolver gran parte de los requisitos necesarios para la integración de la firma digital con Alfresco, se sigue trabajando en el desarrollo de una solución más "ligera" capaz de integrarse con herramientas existentes dedicadas a ello.[24]

Por otra parte los pasos de avance más grande en cuanto a la integración de Alfresco con una PKI ha sido sin dudas la integración del mismo con la herramienta Sinadura Desktop. Esta solución ha creado un pequeño conector para Sinadura con el albergue y custodia de un servidor documental como es el caso de Alfresco. Esta aproximación no requiere alojar un certificado en el servidor, y además permitirá utilizar todos los dispositivos criptográficos que puede utilizar sinadura, ya sean tarjetas criptográficas o certificados de software.

En el desarrollo del conector se utilizaron una combinación de Web Scripts y Web Services de Alfresco y funcionan para la versión Alfresco 3.x (Community y Enterprise). En estos momentos se tiene pensado desarrollar un módulo de Servicios de Interoperabilidad de Gestión de Contenidos(CMIS por sus siglas en ingles Content Management Interoperability Services) que permitirá la integración con otros gestores documentales como Nuxeo, Filenet, Documentum, OpenText, Oracle UCM o Sharepoint (o cualquier repositorio documental que adopte el estandar CMIS) y dotarle de nuevas funcionalidades.

Actualmente esta integración de Sinadura con Alfresco, tiene funcionalidades tan importantes como:

- Añadir a Alfresco: Esta opción permite añadir en Alfresco aquellos documentos PDF firmados que se tengan seleccionados en Sinadura. Para añadirlos es necesario seleccionar uno o varios PDFs en la ventana principal de Sinadura. Tras pinchar en Añadir seleccionaremos la ruta de subida, navegando por el repositorio y escogiendo un determinado espacio.

- Descargar de Alfresco: La opción descargar permitirá navegar por el repositorio de Alfresco y descargarlos en local con Sinadura. La ventana de navegación mostrará solo los documentos en Alfresco con formato PDF. Los ficheros descargados de Alfresco, se alojan en la carpeta temporal del sistema correspondiente.

- Actualizar en Alfresco: Mediante esta opción se actualizará el contenido de cualquier documento PDF alojado en Alfresco (siempre y cuando se tengan los permisos necesarios). Lo primero que se hace es seleccionar un documento de la ventana de Sinadura. Una vez elegido el documento, se indicará el documento de Alfresco que se quiere actualizar, mediante el componente de navegación de espacios de Alfresco.[25]

- Buscar PDF a partir de palabras claves: Esta opción permitirá buscar en el Alfresco el conjunto de documentos con extensión PDF que respondan a los criterios de búsqueda basados en las palabras claves que el usuario haya introducido.

- Seleccionarlos y descargarlos: Mediante esta opción se permitirá la descarga de los documentos encontrados de manera individual o una selección de los mismos.

- Visualizar sus propiedades (metadatos) en Alfresco: La opción visualizar documentos permitirá la visualización de las propiedades del documento o metadatos del mismo a partir de su ubicación en Alfresco.

Las funcionalidades anteriormente mencionadas que hoy cuenta Sinadura aparecen en la versión que este producto público en febrero de 2011, las mismas convierten a dicho software en una de las herramientas más potentes en la actualidad referentes al trabajo de firma digital y su integración con los gestores de documentos como Alfresco.

1.3. Tecnologías a utilizar en el desarrollo del sistema

1.3.1. Metodologías de desarrollo de software

Rational Unified Process (RUP)

El Racional Unified Process (RUP) es una propuesta de un proceso de desarrollo de software orientado a objetos que utiliza UML para describir un sistema, mejora la productividad del equipo de trabajo y entrega las mejores prácticas del software a todos los miembros del mismo, logrando de esa forma obtener un software de mayor calidad y en tiempo. [26]

RUP como metodología, está enfocada al desarrollo de software orientado a objetos, tipo de programación a utilizar en la implementación del sistema. Es adaptable, lo que permitirá que se realicen los cambios que sean necesarios. El lenguaje recomendado para la modelación del sistema es Unified Modeling Lenguaje (UML), ya que se puede aplicar en el desarrollo de software entregando gran variedad de formas para dar soporte a RUP, además de ser un lenguaje gráfico para visualizar, especificar, construir y documentar un sistema, UML también ofrece un estándar para describir un "plano"del sistema (modelo), incluyendo aspectos conceptuales tales como procesos de negocio y funciones del sistema, y aspectos concretos como expresiones de lenguajes de programación, esquemas de bases de datos y componentes reutilizables [27]. RUP genera gran cantidad de artefactos que permiten tener una amplia documentación del producto. Otra de las características que hacen de RUP una buena elección para utilizar como metodología de desarrollo de software es el ser iterativo lo que permite reducir riesgos y dividir los proyectos en pequeños ciclos o iteraciones a través de cada una de las fases.

La presente investigación al formar parte del desarrollo del GDA eXcriba también define a RUP como metodología de desarrollo de software a utilizar.

1.3.2. Herramientas CASE

Visual Paradigm

Visual Paradigm al igual que Rational Rose también utiliza UML como lenguaje de modelado. Dicha herramienta soporta todos los diagramas UML, siendo esta la primera razón que justifica la selección de la

misma para la modelación del sistema. Además genera documentación del sistema en formato PDF, HTML y Word y permite la generación de código a partir de diagramas. Esta herramienta CASE puede ser utilizada para la modelación de procesos de desarrollo de software que sigan la filosofía de software libre, otra de las razones que justifican su selección.

La misma permite realizar ingeniería tanto directa como inversa, pues a partir de un modelo relacional es capaz de desplegar todas las clases asociadas a las tablas. Además Visual Paradigm soporta múltiples usuarios trabajando sobre el mismo proyecto ya que es colaborativa. Permite el control de versiones y es multiplataforma.

1.3.3. Servidores web

Apache

Apache es gratuito, modular, código abierto y extensible. Está diseñado para ser un servidor Web flexible y potente que puede funcionar sobre varias plataformas y entornos, además de poder ser personalizado con el objetivo de mejorar las necesidades de cada sitio Web. Entre sus características se destacan:

- Multiplataforma, ha sido desarrollado para plataformas (Unix, Linux, MacOSX, Vms, Win32, OS2, etc).
- Su desarrollo ha sido de acuerdo al protocolo HTTP/1.1 normalizado por el W3C (WWW Consortium).
- Modular, puede ser adaptado a diferentes entornos y necesidades, de acuerdo con los módulos de apoyo que proporciona.
- Facilita la integración como "plug-ins"de lenguajes de programación de páginas web dinámicas.
- Brinda soporte para bases de datos, el protocolo de comunicación segura SSL,lenguajes de programación Perl y PHP y demás.
- Open Source.

En la solución se empleará el servidor Web Apache por las características antes mencionadas además de ser la solución que actualmente usa el GDA eXcriba. [28]

1.3.4. Lenguajes de programación

Lenguajes de programación del lado del servidor

Java

Es un lenguaje de programación independiente de la plataforma creado por Sun Microsystems. Está pensado expresamente para una arquitectura cliente/servidor en la que sólo es necesario intercambiar pequeñas porciones de código (llamadas Applets) que son ejecutadas por el cliente [29], esta es una de las características que hacen de java el lenguaje de programación a utilizar, además de que el campo de acción del presente trabajo se resumen sobre soluciones desarrolladas en plataformas J2EE.

También es un lenguaje de programación compatible con diferentes plataformas capaz de otorgar funcionalidades a un sitio Web.

PHP

PHP (acrónimo de "PHP: Hypertext Preprocessor"), es un lenguaje de programación del lado del servidor gratuito e independiente de plataforma, con una gran librería de funciones y mucha documentación. Se escribe dentro del código HTML, lo que lo hace realmente fácil de utilizar. Es independiente de plataforma, puesto que existe un módulo de PHP para casi cualquier servidor web [30]. Al ser un lenguaje libre dispone de una gran cantidad de características que lo convierten en la herramienta ideal para la creación de páginas web dinámicas, es por estas razones que el la integración del sistema con el GDA eXcriba será desarrollada utilizando este lenguaje de programación.

Lenguajes de programación del lado del cliente

JavaScript

El lenguaje Java Script fue creado por Brendan Eich en la empresa Netscape Communications, se utiliza en el desarrollo y diseño de sitios webs, para crear pequeños programas que se insertan en una página web o en programas más grandes orientados a objetos mucho más complejos. Además permite crear diferentes efectos e interactuar con el usuario. La programación en este lenguaje está centrada en describir objetos, escribir funciones que respondan a movimientos del mouse, utilización de teclas, cargas de páginas entre

otros [31]. No requiere de compilación ya que el lenguaje funciona del lado del cliente. Estas características hacen que este sea el lenguaje a utilizar para la programación de la interfaz destinada al cliente.

1.4. Conclusiones parciales

Como resultado de la investigación y el análisis bibliográfico realizado, a lo largo de este capítulo, han sido expuestos los principales puntos de interés relacionados con las PKI. Se elaboró el marco teórico que permitirá dar paso a la propuesta de integración que responderá a los objetivos del presente trabajo. Además, se trataron los aspectos relacionados con el objeto de la investigación y sus principales tendencias. Se definieron las metodologías de desarrollo del software y herramientas que se utilizarán en el desarrollo de la solución que se propone, teniendo como resultado las siguientes:

- Metodología de desarrollo de software: Proceso Unificado de Desarrollo (RUP por sus siglas en inglés Rational Unified Process)
- Herramienta CASE: Visual Paradigm
- Servidores Web: Apache
- Lenguaje de programación: Java, PHP, JavaScript
- Entorno de desarrollo: NetBeans

Después de la realización de un estudio sobre las presentes herramientas y metodologías, además de los principales aspectos que abarcarán en el presente trabajo, quedan sentadas las bases para el desarrollo del módulo que forma parte de la propuesta de solución.

Capítulo 2

Capítulo 2: Propuesta de solución

En el presente capítulo se describen detalladamente las características que debe tener el sistema para garantizar la integración del GDA eXcriba con una PKI. Se aborda también, una panorámica del objeto de automatización que formará parte de la solución que se propone, y se describe el modelo de dominio. Se presenta la propuesta de solución que permitirá la integración, y se detallan los requisitos tanto funcionales como no funcionales que debe tener el módulo que formará parte de la misma. Se definen los actores que participan en el mismo y las relaciones que existen entre ellos, se modela el diagrama de casos de uso del sistema y se describen textualmente dichos casos de uso.

2.1. Análisis de la propuesta

La integración de un gestor de documentos, como es el caso de eXcriba, con una PKI, provee al mismo de funcionalidades vitales para la seguridad de la información como el firmado de los documentos que este gestiona y la verificación de dichas firmas digitales. A partir de estas dos funcionalidades principales, se derivan otras que forman parte de los procesos de firmado y verificación de la firma digital, como son la comprobación de la validez de certificados haciendo uso de la CRL publicada por la CA y la sincronización de la herramienta de firmado con una Autoridad de Sellado de Tiempo previamente definida por la CA.

En el capítulo anterior se realizó un acercamiento a las soluciones que hoy permiten la integración de los gestores de documentos, como Alfresco, con infraestructuras de clave pública. Una de las soluciones que en la actualidad brinda mayor cantidad de funcionalidades una vez realizada la integración, es la utilización del software Sinadura Desktop. En febrero del año en curso, el proyecto Sinadura, publicó una actualización de su producto el cual incluía funcionalidades que permiten desde la propia aplicación; añadir documentos a Alfresco una vez que estos hayan sido firmados, o actualizarlos si ya se encontraban almacenados y se desea proceder a la firma de los mismos, la búsqueda de documentos con extensión pdf a partir de palabras

claves y una vez que se obtenga el resultado de la búsqueda, existen opciones como seleccionarlos y descargarlos, permite además visualizar las características de los documentos almacenados en Alfresco a partir de sus metadatos.

Sinadura Desktop es una aplicación multiplataforma y que tiene como valor agregado el ser una alternativa de codigo abierto, por lo que en un futuro con el apoyo de las comunidades de desarrollo, podrían diseñarse nuevas funcionalidades para el software que lo hagan más potente. El mismo tiene la característica de ser una aplicación de escritorio, por lo que necesita de la instalación de la misma en los ordenadores que funcionan como estaciones cliente del GDA eXcriba. El hecho de ser una aplicación de escritorio surge por la necesidad de mantener la clave privada del usuario en su poder y que no viaje por la red, pues sería entonces una debilidad de la seguridad y estaría vulnerable a diferentes tipos de ataques, como la suplantación de identidad, la reactuación o la modificación de archivos. Las características mencionadas hacen que se proponga a Sinadura Desktop como propuesta para la integración del GDA eXcriba con una PKI, dando cumplimiento a la necesidad de firmar documentos. Haciendo uso del presente software se contará además con el complemento del resto de las funcionalidades anteriormente descritas.

Aún cuando Sinadura Desktop agrega funcionalidades capaces de dar cumplimiento a algunas de las necesidades del cliente, como incorporar la firma digital a algunos documentos y es una parte importante de la propuesta de solución que se realiza, todavía existen acotaciones necesarias para una completa integración con el GDA eXcriba. El hecho de que sea una aplicación de escritorio y necesite estar instalada en el ordenador cliente, se convierte hasta cierto punto en una limitante. Cuando un usuario final necesite verificar la firma digital de un documento almacenado en eXcriba, y no posee dicho software instalado, se verá imposibilitado de saber si maneja o no con información auténtica y válida. Es por ello la necesidad de crear un módulo que responda a la verificación de la firma digital desde el servidor de eXcriba y no desde la PC cliente. El módulo que se propone para su implementación teniendo como entrada elementos que proporciona la CA, como es el caso del certificado raíz de la misma, la CRL que esta pública periódicamente, y los certificados que emite, deberá ser capaz de verificar la autenticidad de los documentos firmados que se encuentren almacenados en el GDA eXcriba.

Para concretar la propuesta de solución y darle respuesta al objetivo de la presente investigación se definen dos líneas principales para la integración:

- Integrar el GDA eXcriba con el software Sinadura Desktop para el firmado de los documentos desde las PC cliente.
- Desarrollar un módulo (libPKI) para la verificación de la firma digital a nivel de servidor.

A partir de estas dos directrices de trabajo y teniendo en cuenta que el software Sinadura Desktop ya cuenta con una la suficiente ayuda y manuales de configuración del producto, en el presente trabajo de diploma se centrarán todos los esfuerzos en lograr validar la propuesta a partir de la implementación del módulo libPKI, que se propone para la integración.

2.2. Objeto de automatización

Para la integración del GDA eXcriba con una PKI, se desarrollará un módulo que permitirá automatizar la verificación de la autenticidad de los documentos basándose en la firma digital de los mismos, logrando así la confidencialidad e integridad en la gestión de los documentos a nivel del servidor, sin la necesidad de que el usuario tenga una aplicación en su ordenador como Sinadura Desktop.

2.3. Propuesta del módulo libPKI

Con el propósito de dar cumplimiento al problema planteado se propone el desarrollo de un módulo que se pueda integrar al GDA eXcriba, permitiendo la verificación de la autenticidad, confidencialidad e integridad de los documentos, a nivel de servidor.

El módulo propuesto en la presente investigación está desarrollado sobre plataforma java, haciendo uso principalmente de las librerías BouncyCastle e iText del propio lenguaje. El mismo será parte de la aplicación eXcriba y tendrá su ubicación en la web por lo que no necesitará de su instalación y será de fácil acceso a los usuarios. Durante el funcionamiento del mismo existirá interacción con un almacén de claves que se encuentra en el servidor de Alfresco, específicamente en el sistema de ficheros, en el mismo se almacenarán los Certificados Digitales de los usuarios que hayan firmado los documentos archivados. Estos certificados serán necesarios para el funcionamiento de la aplicación. El sistema permitirá la verificación de la autenticidad de un documento almacenado en el GDA eXcriba a partir de su firma digital,

de igual forma podrá notificar si los certificados asociados al documento son válido para la CA, o si los mismo se encuentran en el Listado de Certificados Revocados publicados por la CA de la entidad. Basándose en estas características el sistema deberá ser capaz de notificar si el documento ha sido modificado o no después de su creación, o si la firma del mismo continúa siendo valida para la entidad.

2.4. Modelo de dominio

No se realiza la modelación del negocio porque debido a la relativa simplicidad del entorno donde esta enmarcado el sistema y el conocimiento que se posee acerca de su funcionamiento, no es necesario realizar el modelo de negocio completo para comprender la problemática que ha de resolverse, siendo suficiente realizar un modelo de dominio o conceptual.

El Modelo de Dominio (o Modelo Conceptual) es una representación visual de los principales conceptos u objetos del mundo real, significativos para un problema o área de interés. Este es de gran ayuda para desarrolladores y usuarios, ya que de esta forma utilizan un vocabulario común y pueden entender el contexto en que se enmarca el sistema.[32]

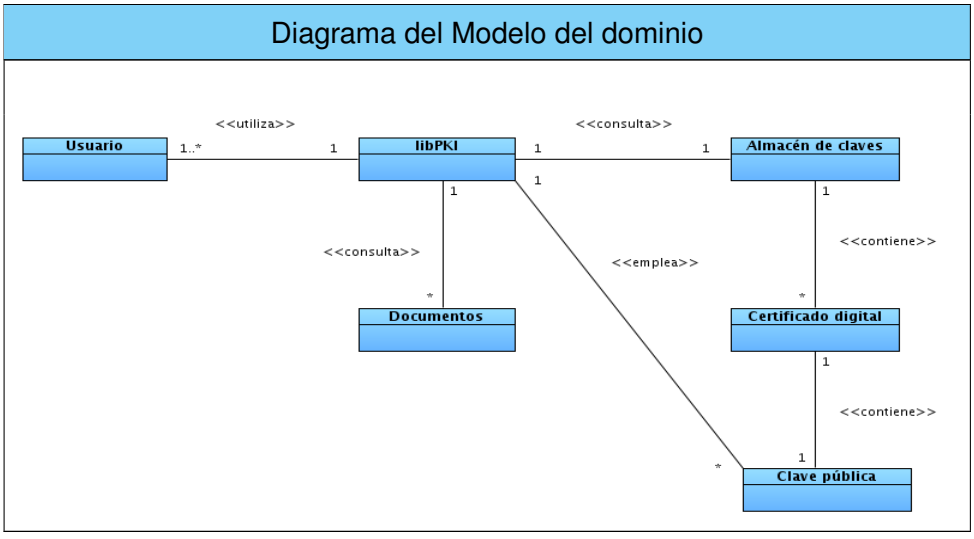

Figura 2.1: Diagrama del Modelo del dominio

Definición de las clases del Modelo de Dominio

Usuario: Persona que interactúa con el sistema, hace papel de actor en el mismo y es iniciador de los casos de uso del sistema.

libPKI: Módulo propuesto integrado al GDA eXcriba.

Documentos: Son los documentos archivados o por archivar en el GDA eXcriba a los que el usuario necesita realizarle comprobaciones.

Almacén de claves: Almacén local de certificados archivados en una tabla de la forma clave valor, donde la clave será el id del usuario y el valor el certificado del mismo.

Certificado digital: Elemento poseedor de varios datos del usuario entre los que se encuentra la clave pública de un usuario.

Clave pública: Elemento necesario para verificar la firma digital de un documento.

2.5. Especificación de requisitos

2.5.1. Requerimientos funcionales

Los requerimientos funcionales son capacidades o condiciones que un sistema determinado debe cumplir. Seguidamente enumeramos los que se han capturado para el desarrollo de esta investigación.[33]

- **R1.** Verificar la autenticidad de los documentos una vez firmados.
  - **R1.1.** Extraer firmas digitales de los documentos.
  - **R1.2.** Obtiene el certificado asociados a la firma digital.
  - **R1.3.** Verificar certificados en la CRL.
  - **R1.4.** Verificar autenticidad de la firma.

2.5.2. Requerimientos no funcionales

Los requerimientos no funcionales detallan las propiedades o cualidades que el producto debe tener, aumentándole funcionalidad al sistema, pues hacen al producto atractivo, fácil de usar, rápido y confiable los

cuales se encuentran separados por categorías que ahora mencionaremos. [33]

Apariencia o interfaz externa:

- El producto debe ser legible y con los colores de la entidad.
- Los mensajes mostrados al usuario deben seguir los patrones definidos por el GDA eXcriba.

Usabilidad:

- El sistema podrá ser usado de forma fácil por cualquier usuario.
- El tiempo de entrenamiento de los usuarios debe ser como máximo de 24 horas.
- Se utiliza el idioma español para los mensajes y textos de la interfaz.
- El funcionamiento del sistema será intuitivo y requerirá de conocimientos mínimos para su uso.

Accesibilidad:

- La información y las funcionalidades estarán disponibles y el usuario podrá acceder a ellas en todo momento.

Fiabilidad:

- Disponibilidad: Una vez que el sistema esté publicado estará siempre disponible y con la información que solicite el usuario, dependiendo únicamente de la operabilidad del GDA eXcriba.

Rendimiento:

- La aplicación permitirá que múltiples usuarios estén conectados a la vez.
- Los tiempos de respuesta y velocidad de procesamiento de la información serán rápidos, no mayores de 10 segundos para las recuperaciones.

Legales:

- Las herramientas seleccionadas para el desarrollo del producto están respaldadas por licencias libres, bajo las condiciones de software libre.Para la herramienta Visual Paradigm la cual no es libre se utiliza la licencia que que posee la universidad.

- La aplicación y toda la documentación generada pertenecen al grupo de proyecto Gestión Documental y Archivística y a la Universidad de las Ciencias Informáticas.

Software:

- Las PC clientes deben tener instalado el navegador web Mozilla Firefox.
- La PC servidor debe contar con servidor web Apache 2.0.
- La PC servidor debe contar con servidor de aplcaciones Apache Tomcat 6.0.
- La PC servidor debe contar con las librerías de java: BouncyCastle e iText.
- La PC servidor debe contar con el almacén de claves donde se almacenarán los certificados digitales de los usuarios que hayan firmado documentos.

Hardware:

- Procesamiento:
  - El servidor de aplicaciones requiere de 1 CPU Intel Pentium o compatible para su correcto funcionamiento.
  - El servidor de base de datos requiere de 1 CPU Intel Pentium o compatible para su correcto funcionamiento.
- Memoria RAM:
  - El servidor de aplicaciones requiere de 2 Gb para su correcto funcionamiento.
  - El servidor de base de datos requiere de 1 Gb para su correcto funcionamiento.
- Capacidad en disco:
  - El servidor de aplicaciones requiere de 40 Gb disponible para su correcto funcionamiento.
  - El servidor de base de datos requiere de 1 Gb disponible para su correcto funcionamiento.

Soporte:

- Realizar pruebas y mantenimiento necesarias para lograr el mejoramiento y evolución en el tiempo.
- Mantener actualizado el certificado de la CA y la CRL del mismo.

Restricciones de diseño e implementación:

- El sistema se desarrollará utilizando como lenguaje de programación Java y PHP.
- El sistema debe contar con las librerías BouncyCastle e iText de java.
- El servidor debe tener instalado servidor web Apache 2.0.
- El servidor de aplicaciones será Apache Tomcat 6.0.
- El entorno de desarrollo integrado será Netbeans 6.9.
- La interfaces destinadas al cliente, deben de programarse en JavaScript.
- Para la modelación del sistema se utilizará Visual Paradigm 6.4.
- Metodología de desarrollo de software RUP, usando el lenguaje de modelación UML.
- El certificado digital perteneciente a la persona que firmó un documento debe encontrarse en el almacén de claves local.
- Las firmas realizadas a los documentos deben seguir todos los patrones establecidos por la CA.

2.6. Definición de Actores y Casos de Uso

2.6.1. Definición de actores del sistema

Actor	Justificación
Usuario	Es la persona con necesidad de verificar la autenticidad de los documentos digitales.

Tabla 2.2: Definición de actores del sistema

2.6.2. Definición de casos de uso

CU-1	**Verificar autenticidad**
Actor	Usuario
Descripción	Permite al usuario verificar la autenticidad de la firma digital del documento.
Referencias	R1

Tabla 2.3: Definición de caso de uso: Verificar autenticidad

2.6.3. Diagrama de Casos de Uso del Sistema

El diagrama de casos de uso del sistema brinda las funcionalidades que el sistema debe ofrecer para aportar un resultado de valor para sus actores.

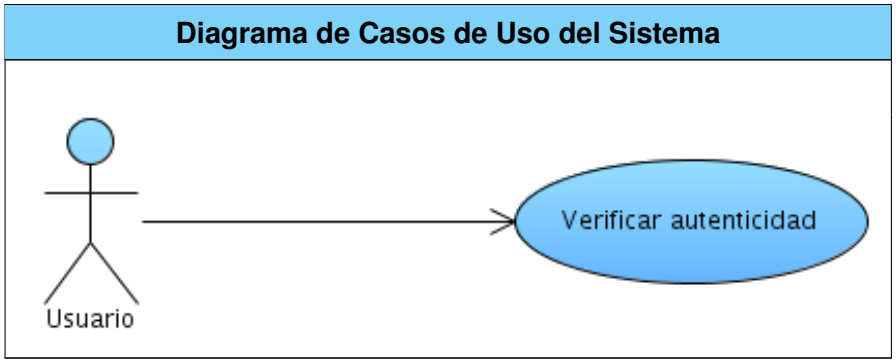

Figura 2.2: Diagrama de Casos de Uso del Sistema

2.7. Descripciones textuales de los casos de uso del sistema

Caso de uso	**Verificar Autenticidad**
Actor	Usuario
	Continúa en la próxima página

Resumen	El caso de uso comienza cuando el usuario decide verificar la autenticidad de la firma digital de un documento y finaliza cuando la misma es verificada correctamente o se muestran las razones por las que la verificación de la misma ha sido insatisfactoria.
Referencias	R1
Precondiciones	El usuario debe estar autenticado en el sistema.
	El documento debe estar firmado siguiendo los patrones establecidos por la CA.
	El certificado digital del autor del documento debe estar en el almacén de claves de la aplicación.
Poscondiciones	

Flujo normal de eventos	
Acción del Actor	**Respuesta del Sistema**
1. El usuario solicita comprobar autenticidad de un documento.	2. El sistema obtiene el nodo en el que se encuentra el documento.
	3. Extrae del documento las firmas digitales que el mismo contiene.
	4. Comprueba que cada una de las firmas que se encuentran en el documento tengan asociado el certificado digital de la autoridad certificadora.
	5. Comprueba que el certificado del autor del documento no se encuetra en la lista de certificados revocados emitida por la autoridad certificadora.

Continúa en la próxima página

	6. Obtiene el certificado digital del autor del documento.
	7. Verifica la autenticidad de la firma digital.
	8. Muestra un mensaje al usuario con el resultado de la verificación.
	9. Finaliza el caso de uso.
Flujo Alterno	
4.a No encuentra el certificado de la autoridad certificadora asociado a la firma digital	
Acción del Actor	**Respuesta del Sistema**
	4.a.1 El sistema muestra un mensaje. Mensaje: El documento no pudo ser verificado. Ausencia de certificado de la CA en la firma digital o certificado del propietario de la firma no presente en el almacén de claves.
	4.a.2 Regresa al paso 1 del flujo normal de eventos.
5.a Encuentra el certificado del propietario de la firma en la lista de certificados revocados emitida por la CA.	
Acción del Actor	**Respuesta del Sistema**
	5.a.1 El sistema muestra un mensaje.
	Mensaje: Error en la verificación. Certificado revocado.
	5.a.2 Regresa al paso 1 del flujo normal de eventos.
6.a No encuentra el certificado del propietario de la firma digital en el almacén de claves.	
Acción del Actor	**Respuesta del Sistema**
	Continúa en la próxima página

	6.a.1 El sistema muestra un mensaje. Mensaje: El documento no pudo ser verificado. Ausencia de certificado de la CA en la firma digital o certificado del propietario de la firma no presente en el almacén de claves.
	6.a.2 Regresa al paso 1 del flujo normal de eventos.
Prioridad	Crítico

Tabla 2.5: Descripción textual del CU: Verificar autenticidad

2.8. Conclusiones parciales

En este capítulo se realizó un estudio de la propuesta de solución que se realizará, definiendo que como aplicación de escritorio que permita el firmado de los documentos se utilizará, Sinadura Desktop, y se implementará un módulo capaz de verificar la firma digital a nivel de servidor. Se mostraron los principales elementos que conforman el dominio del sistema para una mayor comprensión. Se analizaron sus características y funciones fundamentales, las que fueron representadas en el diagrama de casos de uso. Fue identificado el actor que interactúa con el módulo. Se realizó la descripción del caso de uso detallando paso a paso las acciones del actor y las respuestas del sistema y se definieron los requisitos funcionales y no funcionales. Con la culminación de estas acciones quedaron sentadas las bases para comenzar a realizar el análisis y diseño del módulo que se propone para validar la propuesta que se realiza, teniendo en cuenta los requerimientos especificados en el presente capítulo.

Capítulo 3

Capítulo 3: Módulo libPKI

El presente capítulo se centra en los flujos de trabajo, análisis, diseño, implementación y prueba del módulo que se propone como parte de la solución. Se representa mediante un grupo de artefactos la descripción del módulo libPKI, se diagraman las clases del análisis, se elaboran los diagramas de interacción y de clases del diseño utilizando estereotipos webs. También se decribe cómo los elementos del modelo de diseño son implementados en términos de componentes y cómo se organizan de acuerdo con los nodos referidos en el modelo de despliegue. Se exponen las distintas pruebas realizadas al módulo que da solución al caso de uso, aplicando el método de pruebas de caja negra.

3.1. Análisis

3.1.1. Diagrama de clases de análisis

Los diagramas de clases de análisis representan un modelo conceptual temprano que describe las características y comportamiento comunes de un conjunto de elementos que existen en el sistema. Se expresa que es conceptual pues pospone todos los elementos de diseño ya que no considera posibles tecnologías a emplear en el desarrollo del software; constituyen un prototipo de las futuras clases que darán vida al mismo.

A continuación se muestra el diagrama de clases de análisis correspondientes al caso de uso Verificar Autenticidad.

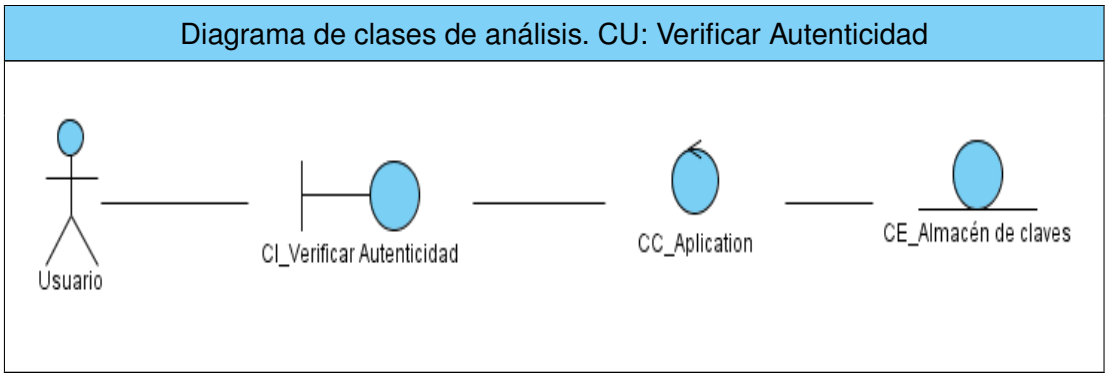

Figura 3.1: Diagrama de clases de análisis. CU: Verificar Autenticidad

3.1.2. Diagrama de interacción

Los diagramas de interacción representan una vista dinámica del sistema y se pueden clasificar en dos tipos, diagramas de colaboración o diagramas de secuencia. Un diagrama de interacción representa la secuencia de acciones que ocurren desde que el actor comienza el caso de uso, así como los mensajes que se envían entre cada una de las clases. En el análisis se usan los diagramas de colaboración, ya que el objetivo principal es identificar las funcionalidades de cada objeto y las responsabilidades sobre ellos.[34]

A continuación se presenta el diagrama de colaboración obtenido en esta investigación.

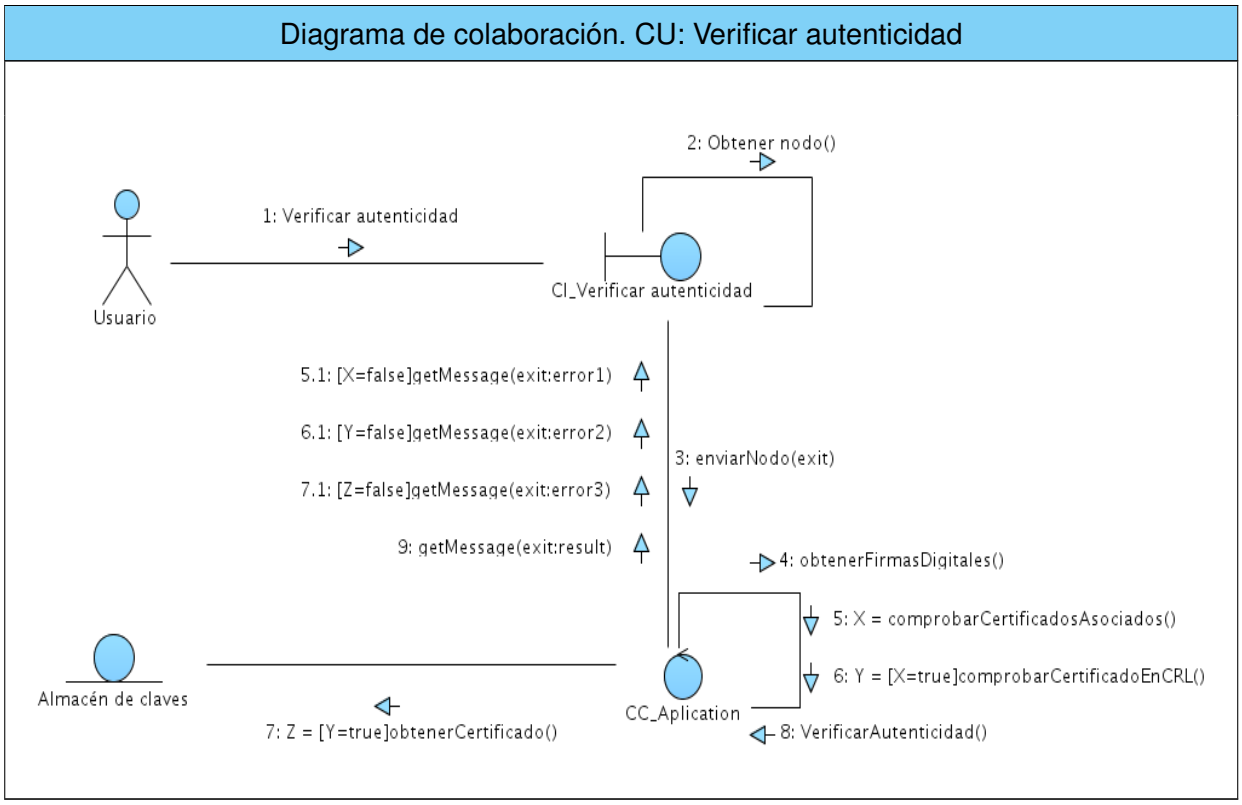

Figura 3.2: Diagrama de colaboración. CU: Verificar autenticidad

3.2. Diseño

3.2.1. Arquitectura del sistema

La arquitectura de software es, a grandes rasgos, una vista del sistema que incluye los componentes principales del mismo, la conducta de esos componentes desde la visión del resto del sistema y las formas en que los componentes interactúan y se coordinan para alcanzar la misión del mismo. La arquitectura de un sistema consiste en la vista conceptual de toda su estructura. [35]

Estilos arquitectónicos

Las soluciones de diseño arquitectónicas que son comunes y reusables a lo largo de años de experiencia se han ido agrupando en lo que más tarde se les llamó estilos. El éxito del diseño de la arquitectura de software depende de los estilos que se decidan utilizar para el desarrollo de la misma. Los estilos expresan la arquitectura en el sentido más formal y teórico, describen entonces una clase de arquitectura, o piezas identificables de las arquitecturas empíricamente dadas. Una vez que se han identificado los estilos, es lógico y natural pensar en reutilizarlos en situaciones semejantes que se presenten en el futuro. [36]

Durante el diseño de la presente investigación se decidió utilizar el estilo arquitectónico, arquitectura en capas, no solo por las facilidades que este ofrece sino también por ser este el estilo definido por el proyecto GDA eXcriba.

Este estilo arquitectónico es un estilo de llamada y retorno, en el mismo cada capa proporciona servicios a la capa superior y se sirve de las prestaciones que le brinda la inferior, al dividir un sistema en capas, cada capa puede tratarse de forma independiente, sin tener que conocer los detalles de las demás. La división de un sistema en capas facilita el diseño modular, en la que cada capa encapsula un aspecto concreto del sistema y permite además la construcción de sistemas débilmente acoplados, lo que significa que si se minimiza las dependencias entre capas, resulta más fácil sustituir la implementación de una capa sin afectar al resto del sistema. [37]

Entre las variantes de la arquitectura en capas la que se decide utilizar es la arquitectura en 3 capas la cual es una especialización muy usada en aplicaciones web donde se observan muy bien delimitadas las responsabilidades de cada capa en la aplicación.

En una arquitectura 3 capas consta de una capa superior que interactúa con una capa inferior mediante interfaces que definen las funcionalidades que la misma debe brindar. Es válido aclarar que todas estas capas pueden residir en un único ordenador, aunque no es esta la práctica más usada, pues lo más común es que exista una multitud de ordenadores donde reside la capa de presentación. Las capas de negocio y de datos pueden residir en el mismo ordenador, y si el crecimiento de las necesidades lo aconseja se pueden separar en dos o más ordenadores. Así, si el tamaño o complejidad de la base de datos aumenta, se puede separar en varios ordenadores los cuales recibirán las peticiones del ordenador en que resida la capa de negocio. Si por el contrario fuese la complejidad en la capa de negocio lo que obligase a la separación, esta

capa de negocio podría residir en uno o más ordenadores que realizarían solicitudes a una única base de datos. En sistemas muy complejos se llega a tener una serie de ordenadores sobre los cuales corre la capa de acceso a datos, y otra serie de ordenadores sobre los cuales corre la base de datos. [38]

En la arquitectura en 3 capas utilizada en la presente investigación se definieron las capas: presentación (Interfaz de usuario), lógica de negocio o dominio (tareas y reglas que rigen el proceso), acceso a datos o gestión de datos (mecanismos de almacenamiento persistente).

Cada una de las cuales encapsula los siguientes elementos:

- Capa de presentación: Es la que interactúa directamente con el usuario, captura la información entrada por éste y hace las peticiones a la capa inferior mostrando al usuario la respuesta proveniente de ésta. Únicamente se comunica con la capa de lógica de negocio.
- Capa de lógica de negocio: Está conformada por los paquetes que integran el sistema, los cuales se ajustan a los requisitos funcionales arquitectónicamente significativos y a los requisitos no funcionales. Desde el punto de vista del diseño, esta capa es contenedora de las clases entidades y controladoras. Se comunica con la capa de acceso a datos y brinda información a la capa de presentación.
- Capa de acceso a datos: Contiene componentes que interactúan con las base de datos y permiten, utilizando los procedimientos almacenados y generados previamente, realizar todas las operaciones con las bases de datos de forma transparente para la capa de negocio.

3.2.2. Patrones del Diseño

Patrones GRASP

Entre los patrones más usados en el mundo de desarrollo de software se encuentran los Patrones de Software para la Asignación General de Responsabilidades(GRASP, por su siglas en inglés General Responsability Assignment Software Patterns), los cuales se dividen en dos grupos, 5 principales (Bajo Acoplamiento, Alta Cohesión, Experto, Creador y Controlador) y 4 de apoyo (Polimorfismo, Fabricación Pura, Indirección y No hables con extraños). En este apartado solo se pretende analizar los patrones que se espera que sirvan de ayuda en el diseño de la propuesta.[39]

Bajo Acoplamiento

Este patrón es un principio que asigna la responsabilidad de controlar el flujo de eventos del sistema, a clases específicas. Esto facilita la centralización de actividades (validaciones, seguridad). El controlador no realiza estas actividades, las delega en otras clases con las que mantiene un modelo de alta cohesión. Un error muy común es asignarle demasiada responsabilidad y alto nivel de acoplamiento con el resto de los componentes del sistema. Durante el trabajo realizado con las clases del diseño se manifestó la presencia de este patrón pues exsiten pocas relaciones entre las clases lo que demuestra que existen muy pocas dependencias y cada clase realiza sus funciones sin necesidad de otras.

Controlador

El patrón controlador sirve como intermediario entre una determinada interfaz y el algoritmo que la implementa, de tal forma que es la que recibe los datos y la que los envía a las distintas clases según el metodo llamado. Este patrón se pone de manifiesto cuando la clase VerifySignature recibe los datos enviados desde la interfaz eXcriba y los envía a la clase DataPKI la cual es la encargada del manejo de la información.

3.2.3. Diagrama de clases del diseño

En la fase de elaboración de la metodología RUP se comienza con un análisis de los elementos significativos de la arquitectura como parte de la primera iteración de elaboración y en las siguientes iteraciones se refina la arquitectura hasta diseñar todos sus elementos. El diseño es el centro de atención al final de la fase de elaboración y el comienzo de las iteraciones de construcción. Esto contribuye a una arquitectura estable, sólida y crea un plano al modelo de implementación.

En el diseño se confeccionan los diagramas de clases del diseño. Los elementos básicos que se pueden encontrar en este diagrama son clases y las relaciones que existen entre las mismas.[40]

A continuación se representa el diagrama de clases de diseño correspondiente al caso de uso Verificar Autenticidad descrito anteriormente.

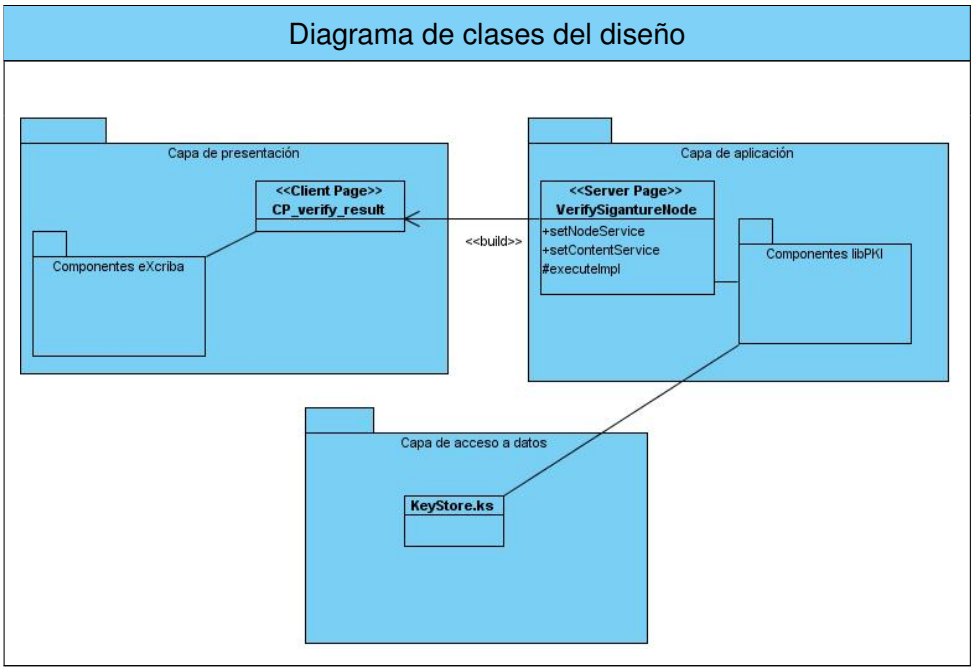

Figura 3.3: Diagrama de clases del diseño

En el diagrama se muestran las relaciones existentes entre las clases archivos o componentes de cada una cada una de las capas. En la capa presentación se encuentra la interfaz de eXcriba, la cual cuenta entre las acciones que muestra al usuario "Verificar Autenticidadrepresentada por la pagina cliente CP_verify_result. Esta clase es contruida por la pagina servidora VerifySignatureNode, la cual se encarga de controlar el proceso de verificación de firma digital que se desarrolla en la capa de negocio. Durante este proceso es necesario consultar la información contenida en el almacén de claves.ks, fichero de informacion que se encuentra en la capa de acceso a datos.

3.3. Implementación

3.3.1. Diagrama de despliegue

En el diagrama de despliegue se muestra cómo y dónde se desplegará el sistema. Las máquinas físicas y los procesadores se representan como nodos, y la construcción interna puede ser representada por

nodos o artefactos embebidos. Los estereotipos permiten precisar la naturaleza del equipo: dispositivos, procesadores y memoria.[41]

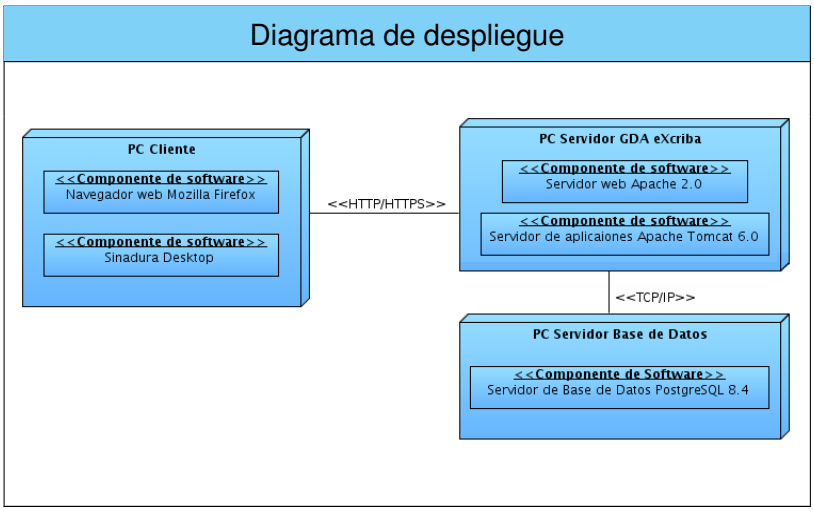

Figura 3.4: Diagrama de despliegue

Descripción del diagrama de despliegue

El diagrama de despliegue representado muestra la siguiente distribución:

- PC_Cliente: Ordenador cliente capaz de conectarse al servidor de aplicaciones mediante el protocolo de comunicaciones HTTP/HTTPS.
- PC_Servidor GDA: Ordenador en que se encuentra el servidor web Apache y el ECM Alfresco, este será el lugar en que se gestione todo el contenido de la aplicación. El mismo establecerá comunicación con los ordenadores clientes mediante protocolo HTTP/HTTPS y con el servidor de base de datos por medio del protocolo TCP/IP.
- Servidor_BD: Ordenador en que se encuentra el gestor de base de datos PostgreSQL capaz de mantener persistente la información generada y a utilizar por la aplicación. El mismo establece comunicación con el servidor GDA usando el protocolo TCP/IP.

3.3.2. Diagrama de componentes

Los diagramas de componentes representan todos los tipos de elementos software que entran en la confección de aplicaciones y las dependencias entre ello. El diagrama de componente forma parte de la vista física de un sistema, la cual modela la estructura de implementación de la aplicación por sí misma, proporcionando la oportunidad de establecer correspondencias entre las clases y los componentes de la implementación. [42]

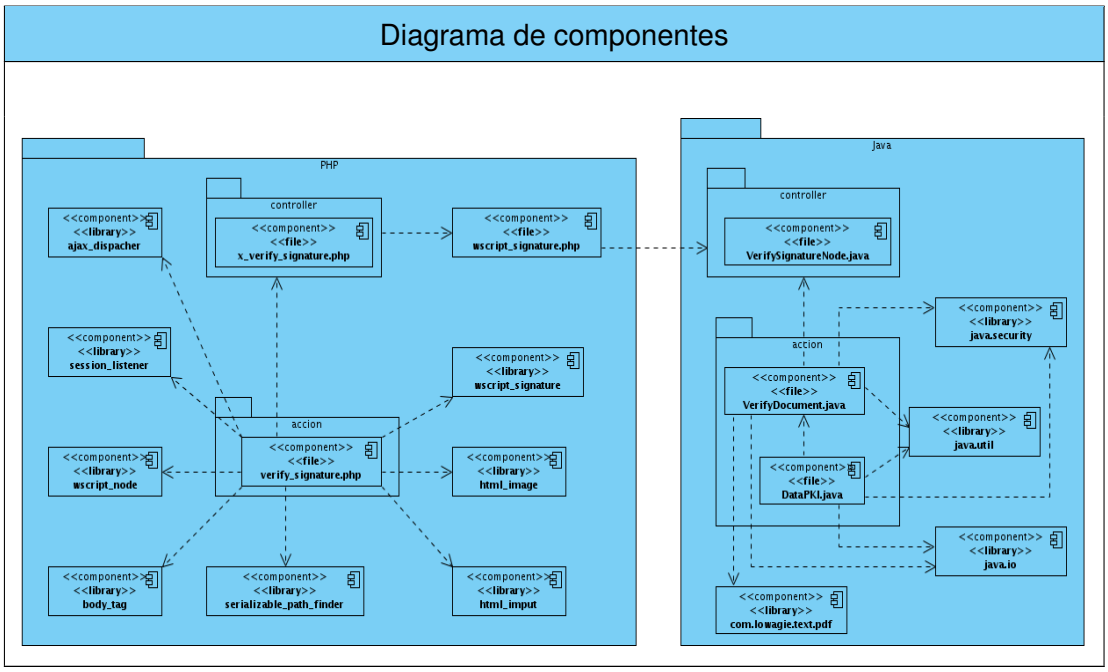

Figura 3.5: Diagrama de componentes

3.3.3. Descripción de componentes

Son varios los componentes representados en el diagrama anterior, pero por su importancia en el desarrollo del módulo libPKI se hace indispensable la descripción detallada de algunos de ellos. Los cuales dan respuesta a los requisitos funcionales definidos previamente. A continuación se representa la descripción de los componentes VerifyDocument.java y DataPKI.java, los cuales representan clases implementadas en lenguaje JAVA y que dan solución al proceso de verificar firma digital.

Descripción del componente VerifyDocument.java

Nombre: VerifyDocument	
Tipo de clase: Controladora	
Atributo	**Tipo**
properties	PropertiesReader
PDF	PdfReader
Para cada responsabilidad:	
Nombre:	VerifyDocument(String pathPDF)
Descripción:	Inicializa los atributos de la clase.
Nombre:	void PKIManager()
Descripción:	Inicializa el atributo properties.
Nombre:	PdfReader readPDF(String path)
Descripción:	Retorna un PdfReader a partir de una dirección dada.
Nombre:	String VerifyDigitalSignature()
Descripción:	Retorna el resultado de la verificación de la firma digital.

Tabla 3.6: Descripción del componente VerifyDocument.java.

Descripción del componente DataPKI.java

Nombre: DataPKI	
Tipo de clase: Controladora	
Atributo	**Tipo**
properties	PropertiesReader
PATH_CACer	String
PATH_CACrl	String

Continúa en la próxima página

PATH_KeyStore	String
PASSWORD_KeyStore	String
Para cada responsabilidad:	
Nombre:	DataPKI()
Descripción:	Inicializa los atributos de la clase.
Nombre:	void PKIManager()
Descripción:	Inicializa el atributo properties.
Nombre:	Certificate getCertificateCA()
Descripción:	Retorna el certificado de la Autoridad Certificadora de la entidad, (el certificado debe estar encontrarse en el almacén de claves.
Nombre:	Certificate getCertificate(String path)
Descripción:	Retorna un certificado digital a partir de una dirección.
Nombre:	Collection getCRL()
Descripción:	Retorna la Collection contenedora de la Lista de Certificados Revocados(CRL) de la Autoridad Certificadora.
Nombre:	KeyStore getKeyStore()
Descripción:	Retorna el almacén de claves local con los certificados y alias que este contiene. De no exsitir el almacén de claves entonces lo crea.
Nombre:	void setKeyStore(String alias, Certificate cer)
Descripción:	Retorna el almacén de claves local con los certificados y alias que este contiene. De no exsitir el almacén de claves entonces lo crea.

Tabla 3.7: Descripción del componente VerifyDocument.java.

3.4. Pruebas

En el desarrollo de un software, el proceso de prueba es clave a la hora de detectar errores o fallas. Las pruebas son de gran importancia en la garantía del software, una selección cuidadosa de los datos de prueba puede ofrecer mucha confianza en cuanto al desempeño que posee el programa. Esto, asociado a un determinado mecanismo de comprobación de errores, puede producir software más confiable. El objetivo principal de la realización de pruebas es descubrir la mayor cantidad posible de defectos del software.[43]

3.4.1. Pruebas aplicadas

Para comprobar la calidad del producto desarrollado, se realizarán pruebas de caja negra, con el objetivo de demostrar que el mismo cumple con los requisitos previamente definidos. En la realización de esta prueba la técnica a emplear será de partición de equivalencia, pues la misma permite examinar los valores válidos e inválidos de las entradas existentes en el software.

A continuación se describe los casos de prueba desarrollados para el caso de uso definido, especificando la información de entrada, los resultados obtenidos una vez ejecutado el caso de prueba y las condiciones que deben cumplirse mientras este se ejecuta.

CP1: Verificar autenticidad de la firma digital		
Entrada	**Resultados**	**Condiciones**
El usuario selecciona la opción “Verificar autenticidad”	El sistema muestra el mensaje: *Documento firmado correctamente. Nombre de la firma: [Signature 1]. Documento firmado por: [Joelsy Porven Rubier]. Fecha de firmado: [2011-02-11: 06:24].*	○ Documento firmado siguiendo los patrones definidos por la CA. ○ Certificado digital de [Joelsy Porven Rubier] se encuentra en el almacén de claves de la aplicación.
Continúa en la próxima página		

El usuario selecciona la opción “Verificar autenticidad”	El sistema muestra el mensaje: *El documento no pudo ser verificado. Ausencia de certificado de la CA en la firma digital o certificado del propietario de la firma no presente en el almacén de claves.*	○ Existen firmas en el documento que no tienen asociado el certificado de la CA.
El usuario selecciona la opción “Verificar autenticidad”	El sistema muestra el mensaje: *El documento no pudo ser verificado. Ausencia de certificado de la CA en la firma digital o certificado del propietario de la firma no presente en el almacén de claves.*	○ El certificado del propietario de alguna de las firmas digitales que aparece en el documento no se encuentra registrado en el almacén de claves.
El usuario selecciona la opción “Verificar autenticidad”	El sistema muestra el mensaje: *Error en la verificación. Certificado revocado.*	○ El certificado del propietario de alguna de las firmas que aparece en el documento se encuentra en la lista de certificados revocados publicada por la CA.
Continúa en la próxima página		

El usuario selecciona la opción “Verificar autenticidad”	El sistema muestra el mensaje: *Existieron problemas durante la comprobación de la autenticidad del documento. Verifique que el documento fue firmado siguiendo las políticas definidas por la Autoridad Certificadora de la entidad.*	○ Existieron problemas al verificar la autenticidad del documento, incompatibilidad de la firma del mismo con el certificado digital almacenado en el almacén de claves.
El usuario selecciona la opción “Verificar autenticidad”	El sistema muestra el mensaje: *Documento no firmado*	○ El documento no ha sido firmado.

Tabla 3.8: CP1: Verificar autenticidad de la firma digital

3.5. Conclusiones parciales

En el presente capítulo se mostraron los diagramas de clases tanto del análisis como del diseño, así como el diagrama de colaboración correspondiente al caso de uso del módulo que se desarrolló durante la presente investigación. La generación de algunos artefactos relacionados con el flujo de análisis y diseño, permitió obtener una mayor comprensión del módulo, así como definir los principios que guiaron la implementación del mismo. Tomando como punto de partida el diagrama de componentes realizado, se obtuvo una visión mucho más clara sobre la estructura del módulo libPKI. Se representó el diagrama de despliegue con los nodos necesarios que garantizaron el correcto despligue del GDA eXcriba con la incorporación del módulo que se propone y se describieron el conjunto de pruebas que se le realizaron a la aplicación.

Conclusiones

De manera general en la presente investigación se desarrolló un módulo capaz de integrar el Gestor de Documentos Administrativos eXcriba con una PKI, permitiendo la verificación de la firma digital de los documentos firmados y archivados en el Gestor de Documentos Administrativos, eXcriba. Entre otros aspectos significativos que apoyaron el desarrollo de la presente investigación podemos destacar que:

- Se realizó un estudio de las herramientas utilizadas en la actualidad para la integración del Gestor de Contenido Empresarial Alfresco con infraestructuras de clave pública, definiéndose Sinadura Desktop como parte fundamental de la propuesta de integración que se realiza.
- Se desarrolló el módulo libPKI para complementar la propuesta de integración, permitiendo verificar la firma digital de los documentos almacenados en el GDA eXcriba, directamente desde la aplicación web.
- Se validó el funcionamiento del módulo propuesto a través del método de caja negra aplicando la técnica de particiones equivalentes, comprobando que el mismo fuera capaz de verificar la firma digital de los documentos .

Recomendaciones

Los resultados obtenidos durante el desarrollo de este trabajo han sido los esperados y de acuerdo a los objetivos que fueron definidos se puede afirmar que a todos los requisitos capturados fueron cumplidos.

No obstante para futuras investigaciones y proyectos que guarden relación con la presente investigación se recomienda:

- Lograr la descarga de los certificados digitales no presentes en el almacén de claves de la aplicación de forma dinámica.
- Integrar el software Sinadura Desktop con el GDA eXcriba.

Glosario de términos

A

Alfresco Gestor de Contenido Empresarial de código abierto, pág. VIII.

C

CASE Computer Aided Software Engineering (Ingeniería de Software Asistida por Ordenador), aplicaciones informáticas destinadas a aumentar la productividad en el desarrollo de software reduciendo el coste de las mismas en términos de tiempo y de dinero, pág. VIII.

certificado Acreditación emitida por una entidad o un particular debidamente autorizados garantizando que determinado dato (por ejemplo, una firma electrónica o una clave pública) pertenece realmente a quien se supone, pág. 13.

certificado digital También conocido como certificado de clave pública o certificado de identidad es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y una clave pública, pág. 3.

confidencialidad Característica de la información por la que la misma sólo puede ser revelada a los usuarios autorizados, pág. VII.

criptografía Término formado a partir del griego kruptos, oculto. La Real Académia lo define como *arte de escribir con clave secreta o de modo enigmático*, pág. 3.

D

DNS Domain Name System o DNS (en castellano: sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada, pág. 19.

F

framework Plataformas o herramientas del mundo de la informática que le proveen a los programadores un grupo de facilidades en el ámbito para la cual han sido creadas, pág. 5.

G

GDA Gestor de Documentos Administrativos: Grupo de trabajo perteneciente al departamento de Gestión Documental y Archivo, pág. VII.

H

hardware Corresponde a todas las partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado. Es el substrato físico en el cual existe el software, maquinaria real. El hardware abarca todas las piezas físicas de un ordenador (CPU, placa base, maquinaria real, cables, transistores, y circuitos), pág. VII.

HTML HyperText Mark Language: Lenguaje de Marcas de Hipertexto. Es el lenguaje de marcado predominante para la construcción de páginas Web.

HTTP HyperText Transfer Protocol: Es el protocolo que emplea la WWW. Define como se tienen que crear y enviar los mensajes y que opciones debe tener el servidor y el navegador en respuesta a un comando.

HTTPS Protocolo Seguro de Transferencia de Hipertexto. Garantiza la seguridad de las comunicaciones entre el usuario y el servidor web al que este se conecta.

I

IDE Integrate Development Enviroment: Entorno de desarrollo integrado. Herramienta que se usa para facilitar el desarrollo de software.

P

PKI Infraestructura de Clave Pública o Public Key Infrastructure. Es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas, pág. VII.

R

Repositorio El repositorio podría definirse en el dominio de las herramientas CASE como la base de datos fundamental para el diseño; no sólo guarda datos, sino también algoritmos de diseño y, en general, elementos software necesarios para el trabajo de programación. En el dominio de las PKI un repositorio sería el lugar en que se almacenan los certificados digitales contenedores de la clave pública, pág. 16.

S

software Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora, pág. VII.

U

UCI Universidad de las Ciencias Informáticas, pág. 1.

UIT Unión Internacional de Telecomunicaciones es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, pág. 59.

UIT-T Es el órgano permanente de la UIT que estudia los aspectos técnicos, de explotación y tarifarios y publica normativa sobre los mismos, con vistas a la normalización de las telecomunicaciones a nivel mundial, pág. 19.

UML Unified Modeling Language: Lenguaje de modelado visual que se usa para especificar, visualizar, construir y documentar artefactos de un sistema de software, pág. 24.

Referencias bibliográficas

[1] L. Nayar, “La gestión documental. conceptos básicos..” Article, (20):15, 2010 [Consultado: Marzo 2011].

[2] C. RAE, “Diccionario de la lengua española - vigésima segunda edición.” http://buscon.rae.es/draeI/,. [Consultado: Noviembre 2010].

[3] C. F. Borghello, “Seguridad informática / amenazas lógicas - tipos de ataques.” http://www.segu-info.com.ar/ataques/tipos.htm. [Consultado: Noviembre 2010].

[4] C. Certes NETWORKS, “Certes networks.” http://certesnetworks.com/. [Consultado: Junio 2011].

[5] C. Network WORLD, “Ovum aboga por una regulación que proteja el uso de las redes sociales en la empresa.” http://www.networkworld.es/Ovum-aboga-por-una-regulacion-que-proteja-el-uso-de-las-rede. [Consultado: Junio 2011].

[6] Anon, “Descripción del cifrado simétrico y asimétrico.” http://support.microsoft.com/kb/246071/es. [Consultado: Abril 2011].

[7] Anon, “Sistemas de cifrado asimétrico.” http://www.gnupg.org/gph/es/manual/x212.html. [Consultado: Dciembre 2010].

[8] Anon, “Autoridad certificante de la subsecretaría de la gestión pública.” http://ca.sgp.gov.ar/faq.html. [Consultado: Noviembre 2010].

[9] C. UPV, “¿qué es una firma electrónica : Certificados digitales : Upv.” http://www.upv.es/contenidos/CD/info/711250normalc.html. [Consultado: Noviembre 2010].

[10] Anon, “Seguridad digital - PKI - infraestructura de clave pública.” http://www.seguridaddigital.info/index.php. [Consultado: Mayo].

[11] C. ARTICSOFT, “What is PKI (Public key infrastructure.” http://www.articsoft.com/public_key_infrastructure.htm. [Consultado: Abril 2011].

[12] C. CertiSur S.A., “PKI introduction research CertiSur.” http://www.certisur.com/pki-introduction. [Consultado: Mayo 2011].

[13] C. DNi, “Zonatic - criptografía y esquemas de clave pública - infraestructura de clave pública.” https://zonatic.usatudni.es/es/aprendizaje/aprende-sobre-el-dnie/57-aspectos-tecnicos. [consultado ayer].

[14] G. Álvares Muñoz, “Pki o los cimientos de una criptografía de clave pública.” http://www.iec.csic.es/criptonomicon/susurros/susurros11.html. [Consultado: Dicembre 2010].

[15] webmaster, “Autoridad certificante de la subsecretaría de la gestión pública.” http://www.seguridaddigital.info/index.php. [Consultado: Diciembre 2010].

[16] Y. P. Dominique Dutoit, “Infraestructura de clave pública : definición de infraestructura de clave pública y sinónimos de infraestructura de clave pública (español).” http://diccionario.sensagent.com/infraestructuraa/es-es/. [Consultado: Dicembre 2010].

[17] Anon, “Welcome! - challenge PKI 2003 TSP.” http://www.jnsa.org/mpki/2003. [Consultado: Dicembre 2010].

[18] C. CERES, “CERES > empresas > catálogo > SELLADO DE TIEMPO o TIMESTAMPING.” http://www.cert.fnmt.es/index.php. [Consultado: Dicembre 2010].

[19] C. Scribd, “Seguridad en redes - control de acceso y técnicas criptográficas.” http://www.scribd.com/doc/39394711/Seguridad-en-redes-Control-de-acceso-y-tecnicas. [Consultado: Dicembre 2010].

[20] E. R. Vázquez, “Asesoria informatica - diccionario definiciones informaticas.” http://www.asesoriainformatica.com/definiciones_c.htm. [Consultado Diciembre 2010].

[21] C. Microsoft, “Importar y exportar certificados.” http://technet.microsoft.com/es-es/library. [Consultado: Enero 2011].

[22] Anon, “x509(1): Certificate display/signing utility - linux man page.” http://linux.die.net/man/1/x509. [Consultado: Enero 2011].

[23] H. D. Carrion, “Delitos informaticos – análisis comparativo de firma electrónica.” http://www.delitosinformaticos.com/firmaelectronica/analisis2.shtml. [Consultado: Noviembre 2010].

[24] C. INNOVASOFT New Tecnologic, “INNOVASOFT NT - módulo de alfresco para firma digital (con soporte para DNIe).” http://innovasoft-nt.com/index.php. [Consultado: Mayo 2011].

[25] C. Zylk, “Firma digital y gestion documental con sinadura y alfresco - blog - zylk.net.” http://www.zylk.net/web/guest/web-2-0/blog/-/blogs/firma-digital. [Consultado: Mayo 2011].

[26] “Jacobson, i.; booch, g.; rumbaugh, j., 2000..” . [Consultado: Noviembre 2010].

[27] A. Geraldo, “Diseño y modelación de un proyecto de software. utilizando el lenguaje uml.” http://www.monografias.com/trabajos24/software-uml/software-uml.shtml. [Consultado: Febrero 2011].

[28] Anon, “Welcome to the apache software foundation!.” http://www.apache.org/. [Consultado: Marzo 2011].

[29] Anon, “programación java.”

[30] C. PHP, “Php: Hypertext preprocessor.”

[31] D. Valdés Pérez, “¿qué es javascript?.”

[32] Anon, “Modelo de dominio « tecnología y synergix.” http://synergix.wordpress.com. [Consultado: Marzo 2011].

[33] Anon, “Requerimientos funcionales y no funcionales.” http://www.mitecnologico.com/Main. [Consultado: Marzo 2011].

[34] J. Medina Serrano, “La web de joaquín - UML - diagramas de interacción.” http://jms32.eresmas.net/tacticos/UML/UML06/UML0601.html. [Consultado: Abril 2011].

[35] C. DocIRS, “Arquitectura en capas.” http://www.docirs.cl/arquitectura_tres_capas.htm. [Consultado: Mayo 2011].

[36] Anon, “Diseño arquitectura del software.”

[37] E. González, “capas de la ingenieria de software.”

[38] Anon, “Diseño arquitectura del software.” http://www.mitecnologico.com/Main/Dise%F1o. [Consultado: Junio 2011].

[39] Anon, “Patrones de GRASP.” http://www.adictosaltrabajo.com/tutoriales/tutoriales.php?pagina. [Consultado: Junio 2011].

[40] Anon, “Diseño UML: diagrama de clases.” http://egdamar877.blogspot.com/2009/05/. [Consultado: Abril 2011].

[41] C. Scribd, “Diagrama de despliegue.” http://www.scribd.com/doc/53551175/11/. [Consultado: Mayo 2011].

[42] Anon, “ingenieriasoftwaredos - diagrama de componentes y objetos.” http://ingenieriasoftwaredos.wikispaces.com/Diagrama+de+componentes+y+objetos. [Consultado: Mayo 2011].

[43] Anon, “Prueba.pdf.” http://indalog.ual.es/mtorres/LP/Prueba.pdf. [Consultado: Junio 2011].

Bibliografía

1. Gestión Documental. [Citado: Noviembre 2010]. Disponible en la direccion web: <http://www.gestiondocumental.biz/>

2. GALLÚS.PHP orientado a objeto. [Citado: Noviembre 2010]. Disponible en la direccion web: <http://www.webestilo.com/php/articulo.phtml?art=27>

3. Modelo de Dominio. [Citado: Noviembre 2010]. Disponible en la direccion web: <http://synergix.wordpress.com/2008/07/10/modelo-de-dominio/>

4. Seguridad en la red - Criptografía. [Citado: Noviembre 2010]. Disponible en la direccion web: <http://www.seguridadenlared.org/es/index25esp.html>

5. Seguridad Digital - PKI - Infraestructura de clave pública. [Citado: Noviembre 2010]. Disponible en la direccion web: <http://www.seguridaddigital.info/index.php?option=com-contenttask=viewid=118Itemid=26>

6. Infraestructura PKI Con Certificados Digitales. [Citado: Noviembre 2010]. Disponible en la direccion web: <http://www.scribd.com/doc/55847712/Infraestructura-PKI-Con-Certificados-Digitales>

7. ¿qué es gestión de contenido empresarial?. [Citado: Diciembre 2010]. Disponible en la direccion web: <http://www.herramientasparapymes.com/que-es-ecm-gestion-de-contenido-empresarial.>

8. Diseño. [Citado: Diciembre 2010]. Disponible en la direccion web: <http://eva.uci.cu/mod/resource/view.php?id=14069>

9. Delitos Informaticos – Análisis comparativo de Firma Electrónica. [Citado: Diciembre 2010]. Disponible en la direccion web:

<http://www.delitosinformaticos.com/firmaelectronica/analisis2.shtml>

10. Diccionario de la lengua española - Vigésima segunda edición. [Citado: Diciembre 2010]. Disponible en la direccion web:
<http://buscon.rae.es/draeI/>

11. Capas de la ingenieria de software. [Citado: Diciembre 2010]. Disponible en la direccion web:
<http://alfonsolomas.blogspot.com/>

12. La firma digital. [Citado: Diciembre 2010]. Disponible en la direccion web:
<http://www.tuguialegal.com/firmadigital3.htm>

13. ¿En qué se basa la firma digital?. [Citado: Diciembre 2010]. Disponible en la direccion web:
<http://www.tuguialegal.com/firmadigital2.htm>

14. La arquitectura PKI. [Citado: Diciembre 2010]. Disponible en la direccion web:
<http://www.webtaller.com//maletin/articulos/arquitectura-pki.php>

15. ¿Qué es una Firma Electrónica?. [Citado: Enero 2011]. Disponible en la direccion web:
<http://www.upv.es/contenidos/CD/info/711250normalc.html>

16. Asesoria informatica - Diccionario definiciones informaticas. [Citado: Enero 2011]. Disponible en la direccion web:
<http://www.asesoriainformatica.com/definicionesc.htm>

17. Sistemas de cifrado asimétrico. [Citado: Enero 2011]. Disponible en la direccion web:
<http://www.gnupg.org/gph/es/manual/x212.html>

18. Sistemas de cifrado asimétrico. [Citado: Enero 2011]. Disponible en la direccion web:
<http://www.gnupg.org/gph/es/manual/x212.html>

19. Criptografía y esquemas de clave pública - Infraestructura de clave pública. [Citado: Enero 2011]. Disponible en la direccion web:
<https://zonatic.usatudni.es/es/aprendizaje/aprende-sobre-el-dnie/57-aspectos-tecnicos>

20. PKI o los cimientos de una criptografía de clave pública. [Citado: Enero 2011]. Disponible en la direccion web:
<http://www.iec.csic.es/criptonomicon/susurros/susurros11.html>

21. Patrones de diseño. Análisis y Diseño. Ingenieria del Software. [Citado: Febrero 2011]. Disponible en la direccion web:
<http://www.ingenierosoftware.com/analisisydiseno/patrones-diseno.php>

22. ¿Qué es un Patrón de Diseño?. [Citado: Febrero 2011]. Disponible en la direccion web:
<http://msdn.microsoft.com/es-es/library/bb972240.aspx>

23. Importar y exportar certificados. [Citado: Febrero 2011]. Disponible en la direccion web:
<http://technet.microsoft.com/es-es/library/cc738545(WS.10).aspx>

24. x509. [Citado: Febrero 2011]. Disponible en la direccion web:
<http://linux.die.net/man/1/x509>

25. Sifra consultores S.A. de C.V. [Citado: Febrero 2011]. Disponible en la direccion web:
<http://www.sifra.net.mx/metodologc3ada/microsoft-solution-framework.aspx>

26. Curso de Apache sobre Linux. [Citado: Febrero 2011]. Disponible en la direccion web:
<http://www.ciberaula.com/curso/apache/>

27. Welcome to The Apache Software Foundation. [Citado: Febrero 2011]. Disponible en la direccion web:
<http://www.apache.org/>

28. Nuestra PKI. [Citado: Febrero 2011]. Disponible en la direccion web:
<http://www.ccti.ull.es/ccti/proyectos/web-ull-pki/Pages/estPKI.htm>

29. MySQL. [Citado: Marzo 2011]. Disponible en la direccion web:
<http://www.mysql.com/why-mysql/>

30. Requerimientos Funcionales Y No Funcionales. [Citado: Marzo 2011]. Disponible en la direccion web:
<http://www.mitecnologico.com/Main/RequerimientosFuncionalesYNoFuncionales>

31. Análisis y Diseño de sistemas. [Citado: Marzo 2011]. Disponible en la direccion web:
<http://html.rincondelvago.com/analisis-y-diseno-de-sistemas1.html>

32. INNOVASOFT NT. [Citado: Marzo 2011]. Disponible en la direccion web:
<http://innovasoft-nt.com/index.php?option=com>

33. INNOVASOFT NT - Módulo de Alfresco para firma digital [Citado: Marzo 2011]. Disponible en la direccion web:
<http://www.innovasoft-nt.com/>

34. Autoridad de sellado de tiempo. [Citado: Marzo 2011]. Disponible en la direccion web:
<http://www.hotfrog.es/Empresas/Realsec-Sistemas-de-cifrado-y-firma-digital>

35. Diagramas de interacción. [Citado: Abril 2011]. Disponible en la direccion web:
<http://jms32.eresmas.net/tacticos/UML/UML06/UML0601.html>

36. Diseño Arquitectura Del Software. [Citado: Abril 2011]. Disponible en la direccion web:
<http://www.mitecnologico.com/Main/DiseF1oArquitecturaDelSoftware>

37. INNOVASOFT NT - Productos destacados. [Citado: Abril 2011]. Disponible en la direccion web:
<http://innovasoft-.com/index.php?option=comcontenttask=viewid=54Itemid=203>

38. PKI a los cimientos de una criptografía de clave pública. [Citado: Abril 2011]. Disponible en la direccion web:
<http://www.iec.csic.es/criptonomicon/susurros/susurros11.html>

39. Cómo funcionan las firmas digitales. [Citado: Abril 2011]. Disponible en la direccion web:
<http://www.iec.csic.es/criptonomicon/articulos/expertos32.html>

40. Módulo de Alfresco para firma digital (con soporte para DNIe). [Citado: Mayo 2011]. Disponible en la direccion web:
<http://innovasoft-nt.com/index.phpoption=comcontenttask=viewid=65Itemid=189>

41. PHP: Hypertext Preprocessor. [Citado: Mayo 2011]. Disponible en la direccion web:
<http://www.php.net/>

42. Implementación de una infraestructura de clave pública PKI. [Citado: Mayo 2011]. Disponible en la direccion web:
<http://www.abcdatos.com/tutoriales/tutorial/z8671.html>

43. Paso a paso PKI y certificados digitales - Network World. [Citado: Mayo 2011]. Disponible en la direccion web:
<http://www.networkworld.es/Paso-a-paso-PKI-y-certificados-digitales>

44. Vista general - zylk.net. [Citado: Mayo 2011]. Disponible en la direccion web:
<http://www.sinadura.net/products/sinadura-desktop/overview>

45. Firma Digital Documentos que incluyen Certificado Digital. [Citado: Mayo 2011]. Disponible en la direccion web:
<http://www.informatica-hoy.com.ar/seguridad-informatica/Firma-Digital>

46. Alfresco. View topic - Digital Signature in Alfresco. [Citado: Mayo 2011]. Disponible en la direccion web:
<http://forums.alfresco.com/en/viewtopic.php?t=7991>

47. PKI. [Citado: Mayo 2011]. Disponible en la direccion web:
<http://www.hob.com.mx/html/pki.html>

48. ¿Qué es la firma digital y para qué sirve? . [Citado: Mayo 2011]. Disponible en la direccion web:
<http://www.consumer.es/web/es/tecnologia/internet/2004/01/23/94524.php>

49. Lista de Certificados revocados. [Citado: Mayo 2011]. Disponible en la direccion web:
<http://www.firmadigital.go.cr/revocados.html>

50. Políticas de Certificados. [Citado: Mayo 2011]. Disponible en la direccion web:
<http://www.firmadigital.go.cr/politicas.html>

51. Nuevas funcionalidades para el conector de Sinadura para Alfresco y Nuxeo. [Citado: Junio 2011]. Disponible en la direccion web:
<http://www.sinadura.net/web/guest/web-2-0/blog/-/blogs/nuevas-funcionalidades>

52. Certificados de la Autoridad Certificadora (CA). [Citado: Junio 2011]. Disponible en la direccion web: <http://www.firmadigital.go.cr/ac.html>

53. Firma Digital y PKI. [Citado: Junio 2011]. Disponible en la direccion web: <http://www.macroseguridad.com/index>

54. Grave fallo de diseño en PKI. [Citado: Junio 2011]. Disponible en la direccion web: <http://www.kriptopolis.org/grave-fallo-de-diseno-en-pki-compromete-las-firmas-digitales>

55. Patrones de diseño software. [Citado: Junio 2011]. Disponible en la direccion web: <http://www.proactiva-calidad.com/java/patrones/index.html>

56. Prueba de Programas. [Citado: Junio 2011]. Disponible en la direccion web: <http://www.lab.dit.upm.es/ lprg/material/apuntes/pruebas/testing.htm>

57. PKI. [Citado: Junio 2011]. Disponible en la direccion web: <http://www.scribd.com/doc/36251684/PKI>

58. Seguridad en JAVA: Seguridad en el entorno Java: Ficheros de configuración. [Citado: Junio 2011]. Disponible en la direccion web: <http://www.uv.es/sto/cursos/seguridad.java/html/sjava-37.html>

59. PKI en GNU/Linux. Articulos. Revistalinux.net, Linux, software libre, Ubuntu, programación. [Citado: Junio 2011]. Disponible en la direccion web: <http://revistalinux.net/articulos/infraestructuras-de-clave-publica-kpi-en-gnulinux/>

60. Nuevas funcionalidades para el conector de Sinadura para Alfresco. [Citado: Junio 2011]. Disponible en la direccion web: <http://www.zylk.net/web/guest/web-2-0/blog/-/blogs/nuevas-funcionalidades-para-el-conector>

61. Firma digital y gestion documental con Sinadura y Alfresco. [Citado: Junio 2011]. Disponible en la direccion web: <http://www.zylk.net/web/guest/web-2-0/blog/-/blogs/firma-digital-y-gestion-documental-con-sinadura>