Universidad de las Ciencias Informáticas

Facultad 1

Propuesta de solución para el cifrado de documentos desde el Portafirmas Digit@l

Trabajo de Diploma para optar por el Título de Ingeniero en Ciencias Informáticas

Autor: Mirley Nuez Pupo

Tutores: Ing. Reinier Elejalde Chacon

Ing. Ronny Zamora Aguilar

La Habana, 2012

Declaración de autoría

Declaro que soy el único autor de este trabajo y autorizo al Centro de Informatización Universitaria de la Universidad de las Ciencias Informáticas, para que hagan el uso que estimen pertinente con este trabajo.

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

_____

Firma del autor

Mirley Nuez Pupo

_____

Firma del tutor

Ing. Reinier Elejalde Chacon

_____

Firma del tutor

Ing. Ronny Zamora Aguilar

Resumen

Este trabajo tiene como principal objetivo, proponer una solución para el cifrado de documentos desde el Portafirmas Digit@l que se desarrolla en la Universidad de las Ciencias Informáticas (UCI), mediante técnicas propuestas por la criptografía moderna. Para su cumplimiento se realizó un estudio del estado del arte sobre el tema a tratar y se determinó que se utilizará un mecanismo híbrido de cifrado, que combina los mecanismos simétricos y asimétricos. Además, se definieron los protocolos criptográficos, que representan el orden en que se deben ejecutar los algoritmos de cifrado y las acciones a realizar entre el cliente (Portafirmas Digi@l) y el servidor (Repositorio de contenidos del Portafirmas Digit@l, donde reside la información), para llevar a cabo una comunicación segura.

Palabras clave: criptografía, protocolos criptográficos, sistemas de cifrado.

Índice General

Introducción

La palabra criptografía proviene del griego *krypto* y *grafos*, que significan oculto y escritura respectivamente, por lo que se entiende escritura oculta. En la práctica, la criptografía consiste en aplicar mecanismos – *generalmente matemáticos* – que transformen los mensajes, de manera que solo puedan ser entendidos por aquellas personas que conozcan los procedimientos para volverlos a su forma original.

Históricamente la criptografía ha transitado por tres períodos fundamentales: Pre-científica, Científica y de Clave pública. La criptografía Pre-Científica se caracterizó por ser más un arte que una ciencia, pues los métodos de cifrado que se utilizaban poseían una consistente formulación algebraica, pero carecían de una sólida base matemática. En 1948, con la publicación de la Teoría de la Información por Shannon [1], comienza la etapa de la criptografía Científica, más elaborada y con una amplia base matemática. Finalmente, en el año 1976 se publica el estudio realizado por Whitfield Diffie [2] y Martin Hellman[3] sobre la aplicación de funciones matemáticas de un solo sentido a un modelo de cifra, denominado cifrado con Clave pública[1].

La criptografía, desde sus inicios, ha estado asociada con la protección de la información. En los últimos años, su uso se ha generalizado en los diferentes medios en los que intervienen las tecnologías de la información y las comunicaciones (TIC), con la intención de mantener la información en secreto o velar por su integridad, evitando posibles ataques para destruirla o manipularla. Se considerada el mecanismo más

[1] Claude Elwood Shannon (30 de abril de 1916 - 24 de febrero de 2001), ingeniero electrónico y matemático estadounidense, recordado como «el padre de la teoría de la información».

[2] Whitfield Diffie, en 1965 se graduó de matemático en el Instituto Tecnológico de Massachusetts. En 1976 publicó junto a Martin Hellman "New Directions in Cryptography", convirtiéndose en pionero de la criptografía de clave pública.

[3] Martin E. Hellman, se graduó en la Universidad de Nueva York en 1966 con el título de Ingeniería Eléctrica. Hellman es famoso por ser el inventor junto a Diffie de la criptografía de clave pública.

eficiente para obtener un alto nivel de seguridad en los estados más vulnerables de la información: su transmisión y almacenamiento.

Debido a la diversidad de sistemas de información que gestionan y tramitan información de carácter confidencial, cada vez más, se desarrollan aplicaciones informáticas capaces de facilitar el acceso y obtención de esta, de forma rápida, ágil y eficaz. Una de estas aplicaciones son los portafirmas digitales, se trata de herramientas que utilizan los modelos matemáticos propuestos por las técnicas criptográficas modernas, para llevar a cabo el proceso de autorización y aprobación formal de documentos electrónicos a través de la firma digital [4], con la finalidad de garantizar su autenticidad e integridad.

Siguiendo este principio, en el Departamento de Gestión Documental de la Universidad de las Ciencias Informáticas (UCI) se desarrolla un portafirmas digital: Portafirmas Digi@l. Un elemento de especial interés en la concepción de esta herramienta es garantizar la seguridad de la información que radica en su repositorio de contenidos, se suele pensar que al encontrarse dentro del área de seguridad la información está "suficientemente segura". Sin embargo, si algún atacante viola las políticas y el perímetro de seguridad tendrá acceso pleno a toda la información que reside en el repositorio. Más preocupante aún es que el enemigo sea el administrador del sistema. Estas brechas de seguridad conllevan a los clientes a exigir un sistema de seguridad de alto nivel que responda a las siguientes interrogantes:

- ¿Cómo evitar que los administradores de los servicios/servidores puedan acceder a la información contenida en los documentos almacenados en el repositorio de contenidos del Portafirmas Digit@l?
- ¿Cómo evitar que intrusos que hayan logrado acceder a los servidores o al sistema como administradores, se apoderen de la información contenida en los documentos almacenados en el repositorio de contenidos del Portafirmas Digit@l?

A raíz de la situación problemática anteriormente planteada se formula el siguiente **problema a resolver**: ¿Cómo garantizar la confidencialidad de la información contenida en documentos almacenados en el repositorio de contenidos del Portafirmas Digit@l?

[4] La firma digital incluye en los documentos un código seguro de verificación generado electrónicamente, que permite constatar su integridad y autenticidad.

Para ello el **objeto de estudio** de la presente investigación es la criptografía moderna y el **campo de acción** la criptografía moderna en el cifrado de documentos.

Siendo el **objetivo general**: diseñar un módulo para el Portafirmas Digit@l que a partir de un conjunto de protocolos criptográficos y servicios para la comunicación cliente-servidor, permita distribuir y almacenar en medios inseguros información que en determinados momentos se considera confidencial.

Para dar cumplimiento al **objetivo general** se han establecido los siguientes **objetivos específicos**:

- Definir los requisitos de seguridad que debe disponer la solución.
- Especificar los protocolos criptográficos necesarios para cubrir los requerimientos de seguridad identificados.
- Validar la propuesta.

Como **idea a defender** se plantea que: una solución de cifrado de documentos para el Portafirmas Digit@l, incrementará la seguridad de la información contenida en los documentos a nivel de repositorio de contenidos.

Para llevar a cabo esta investigación se aplicarán los siguientes métodos científicos:

Métodos teóricos:

- **Analítico-Sintético**: se utilizó para el análisis de los conceptos fundamentales de la criptografía moderna, así como de los elementos que la conforman. Una vez obtenido los conocimientos sobre el fenómeno en cuestión se procederá a sintetizar los resultados de la investigación para desarrollar la solución propuesta.
- **Modelado**: mediante este método se crean abstracciones con el objetivo de obtener una mejor comprensión del proceso de cifrado de los documentos, obteniendo una panorámica de las actividades que intervienen en la solución.

Métodos empíricos:

- **Observación**: se utilizó para identificar la situación problemática que da paso al desarrollo de la investigación, así como para realizar una evaluación de los resultados obtenidos con los resultados esperados.

Como **justificación de la investigación** se plantea que: el desarrollo de una solución para el Portafirmas Digit@l que permita cifrar documentos, garantizará que la información plasmada en los documentos no pueda ser leída por otra persona distinta del destinatario final. De manera general, evita que personas no autorizadas obtengan la información almacenada en determinados documentos que se encuentran en el repositorio de contenidos de dicho sistema.

El presente documento se encuentra estructurado en los siguientes capítulos:

- **Capítulo I: Fundamentos teóricos de la criptografía moderna: Los Portafirmas Digitales**: se realiza un estudio sobre los conceptos generales y básicos relacionados con la criptografía moderna. Se analizan algunos Portafirmas Digitales existentes en el mundo con la intención de identificar como estas herramientas hacen uso de los mecanismos criptográficos.

- **Capítulo II : Propuesta de solución**: se documenta la solución propuesta desde el punto de vista conceptual, teniendo en cuenta los requisitos funcionales y no funcionales identificados, así como los casos de usos asociados a estos requisitos. Además, se identifican las posibles herramientas, lenguajes y metodología a utilizar durante el desarrollo de la solución que se propone.

- **Capítulo III: Protocolos criptográficos**: se describe el conjunto de acciones coordinadas a realizar por parte del cliente y el servidor con el objeto de llevar a cabo un intercambio de datos o información de forma segura en el contexto del sistema.

- **Capítulo IV: Análisis y Diseño**: se puntualizan los elementos para llevar a cabo el desarrollo de la solución, se pone de relieve una solución lógica: cómo el sistema cumple con los requerimientos, definiéndose una arquitectura guía.

Capítulo 1

Fundamentos teóricos de la criptografía moderna: Los Portafirmas Digitales

Según el diccionario de la Real Academia criptografía es el *"Arte de escribir con clave secreta o de un modo enigmático"* [2]. Esta definición no es del todo adecuada en la actualidad, ya que la criptografía ha dejado de ser un arte para convertirse en una ciencia, pues tiene bases matemáticas como son: teoría de números, teoría de la complejidad algorítmica, teoría de la información y estadística [3].

La criptografía clásica engloba todos los mecanismos criptográficos utilizados hasta la mitad del siglo XX. El adjetivo de clásica, en contraposición al de criptosistemas modernos se debe a las técnicas utilizadas, compuestas por operaciones de sustitución y transposición de caracteres, siempre unido al concepto de clave secreta. Estos algoritmos utilizaban una matemática elemental, por lo que para comprenderlos no es necesario tener un alto nivel de conocimiento sobre las matemáticas. Sin embargo, constituyen la base teórica para comprender los algoritmos que ofrece la criptografía moderna.

Los algoritmos criptográficos clásicos basados en el cifrado por sustitución establecen una correspondencia única de los símbolos dentro del mensaje. Es decir, si al símbolo A le corresponde el símbolo D, esta asociación se mantiene a lo largo de todo el mensaje. El algoritmo de César, es un ejemplo de este tipo de cifrado, que consiste en sumar 3 a la posición de cada letra en el alfabeto. De esta forma, a la A le corresponde la D, a la B la E, y así sucesivamente [3].

El cifrado por transposición consiste en barajar los símbolos del mensaje original colocándolos en un orden distinto, de manera que el criptograma contenga los mismos elementos del texto claro, pero colocados de manera tal que resulten incomprensibles. Para obtener el texto claro, el receptor, con conocimiento de la transposición, recoloca los símbolos desordenados del criptograma en su posición original [3]. Este tipo de mecanismos de cifrado no sustituye unos símbolos por otros, sino que cambia su orden dentro del texto. Un ejemplo sencillo de cifrado por transposición consiste en escribir al revés las palabras de un texto.

Estudios realizados por Whitfield Diffie y Martin Hellman en 1976, sobre aplicaciones de funciones matemáticas de un solo sentido a un modelo de cifra introducen el concepto de clave pública, que da inicio a la criptografía moderna [4]. La cual se basa en las mismas ideas básicas que la criptografía tradicional, la transposición y la sustitución, pero sus mecanismos de cifrado son más complejos.

La criptografía moderna se divide en los siguientes bloques según la relación existente entre clave de cifrado y de descifrado:

- Mecanismos de claves secretas: solo existe una clave, utilizada para cifrar y descifrar y tiene que ser del conocimiento tanto del emisor como del receptor del mensaje. La seguridad depende de mantener dicha clave en secreto[4].

- Mecanismos de clave pública: las claves no son únicas sino que formas pares, denominadas clave pública y clave privada. El beneficio principal que ofrecen los mecanismos de clave pública es que permiten que personas que no tienen un acuerdo de seguridad previo, puedan intercambiar información de forma segura por canales de comunicación inseguros y la necesidad de enviar y recibir las llaves secretas a través de algún canal seguro es eliminada, puesto que todas las comunicaciones involucran únicamente llaves públicas y ninguna llave privada es transmitida o compartida[4].

En la actualidad, los mecanismos criptográficos constituyen la alternativa más eficiente para garantizar la seguridad de la información, tanto en la transmisión como en su almacenamiento. Su uso se ha generalizado en todos aquellos campos de la vida moderna en los que se necesita mantener la información en secreto o en los que se vela por su integridad.

1.1. Definiciones preliminares

1.1.1. Criptografía

Jorge Ramió Aguirre[1] en su libro ”Seguridad Informática y Criptografía” define la criptografía como: *“Rama inicial de las Matemáticas y en la actualidad también de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves”* [4].

1.1.2. Clave

En criptografía, una clave es un valor que trabaja con un algoritmo criptográfico para producir un texto cifrado; las claves son básicamente números muy grandes, y su tamaño se mide en bits. Cuanto más grande sea la clave más seguro será el texto cifrado. Las claves deben ser almacenadas en forma cifrada para evitar que algún intruso pueda obtenerla [5].

1.1.3. Criptosistema

Un criptosistema de define como una quíntupla (M, C, K, E, D), según [6]:

- **M**: representa el conjunto de todos los mensajes sin cifrar (lo que se denomina texto plano, o plaintext) que pueden ser enviados.
- **C**: representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
- **K**: representa el conjunto de claves que se pueden emplear en el criptosistema.

[1] Dr. Ingeniero de Telecomunicación diplomado por la Universidad Politécnica de Madrid. Creador y coordinador de CriptoRed, la Red Temática Iberoamericana de Criptografía y Seguridad de la Información.

- **E**: es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de **M** para obtener un elemento de **C**. Existe una transformación diferente E_k para cada valor posible de la clave **k**.

- **D**: es el conjunto de transformaciones de descifrado, análogo a **E**.

Los criptosistemas son clasificados como:

Criptosistemas simétricos o de clave secreta: son aquellos que emplean la misma clave k tanto para cifrar como para descifrar.

Criptosistemas asimétricos o de clave pública: emplean una doble clave (Kpriv, Kpub). Kpriv se conoce como clave privada y Kpub se conoce como clave pública. Una de ellas es utilizada para la transformación E de cifrado y la otra para la transformación D de descifrado [6].

1.1.4. Esteganografía

El término esteganografía, que viene del griego stegos (cubierta), significa escritura oculta o escritura encubierta y es el conjunto de técnicas que nos permiten ocultar o camuflar cualquier tipo de datos. Esteganografía y criptografía pueden parecer en un principio términos equivalentes, pero son mecanismos completamente distintos. El objetivo de la criptografía es hacer ininteligible el mensaje, mientras que la esteganografía tiene sus fuerzas en el desconocimiento de su existencia[7].

Una de las primeras y sencillas técnicas esteganográficas fue el uso de la tinta invisible, que consistía en escribir mensajes en un papel con vinagre o zumos de frutas. Al calentar el papel, la escritura oculta se hacía visible. Este método no tiene porqué ser alternativo a la criptografía, ambos pueden ser utilizados de forma simultánea [7].

1.1.5. Criptoanálisis

El criptoanálisis es la ciencia encargada de analizar y romper la comunicación segura. Las técnicas clásicas de criptoanálisis involucran una combinación de razonamiento analítico, la aplicación de

herramientas matemáticas y búsqueda de patrones. La criptografía y el criptoanálisis siempre se han desarrollado de forma paralela, pues cualquier método de cifrado lleva siempre emparejado su criptoanálisis correspondiente. Se encuentra estrechamente vinculado a cada algoritmo de cifrado. Cuando se diseña un criptosistema, es necesario tener en cuenta todos los posibles ataques que puede sufrir. No existe un procedimiento general de criptoanálisis; cada algoritmo es atacado según su estructura.

1.2. Sistemas de cifrado

1.2.1. Sistemas de cifrado simétrico

Los sistemas de cifrado simétrico o también llamados sistemas de clave secreta son los herederos de la criptografía clásica, y se basan en la utilización de un esquema de cifrado con una única clave, que debe ser del conocimiento tanto del receptor como del emisor del mensaje. Se consideran una buena alternativa para proteger información que no interviene en protocolos de comunicación (por ejemplo, cifrado de material reservado en discos duros)[1].

Estos sistemas, además de asegurar la confidencialidad de la información, permiten la autenticación, siempre y cuando la clave permanezca en secreto entre el receptor y el emisor, dado que el receptor puede determinar que el emisor es quien dice ser y no un suplantador, ya que supuestamente son ellos los únicos que conocen la clave. Sin embargo, esta autenticación no tiene valor fuera de los agentes de la comunicación, pues se basa en la confianza mutua, y no puede ser utilizada ante terceros para evitar la repudiación de un mensaje por parte de quien lo ha escrito[1].

Por otro lado, estos sistemas tienen un punto débil: la necesidad de compartir la clave secreta entre emisor y receptor, ya que se tiene que encontrar una forma segura para llegar a un acuerdo común sobre la clave a utilizar, siendo un riesgo en la seguridad del sistema de cifrado. Además, garantizar la seguridad de la clave es un problema en el mundo actual, en el que es necesario comunicarse a distancia con un gran número de personas o empresas con las que no se ha tenido jamás contacto previo[1].

Estos criptosistemas presentan problemas de gestión de claves, debido a que el número de claves secretas requeridas crece mucho con el de personas implicadas en la comunicación. Por cada dos interlocutoras se necesita una clave, por lo que para n interlocutoras el número de claves necesarias sería n∗(n-1)/2. Si una sola de ellas es revelada y ello llega al dominio público, la confidencialidad de la información quedaría comprometida[1].

Además, existe un problema adicional: la responsabilidad compartida en la gestión del secreto de la clave. En este caso, las empresas, que son las mayores interesadas en proteger su información confidencial, no tienen posibilidad de controlar el grado de fiabilidad de sus clientes, que podría revelar su clave (involuntaria o intencionadamente) y luego estos pueden acusar a la empresa de infidelidad en su custodia (para no responsabilizarse de su error o para llevarlas al fracaso) [1].

1.2.2. Sistemas de cifrado asimétrico

Los sistemas de cifrado asimétrico también denominados de clave pública, consisten en la existencia de dos claves distintas: clave privada y clave pública, una se usa para cifrar y la otra para descifrar. A pesar de la estrecha relación que existe entre ambas claves, disponer de una de ellas no permite recuperar la otra. Para realizar un proceso de cifrado asociado a garantizar la confidencialidad de la información, el protocolo criptográfico a utilizar es el siguiente:

1. Alicia desea enviar un mensaje confidencial a Juan, para ello Alicia conoce la clave pública de este último, ya que es de dominio público.

2. Alicia cifra el mensaje utilizando la clave pública de Juan.

3. Alicia envía el mensaje cifrado a Juan.

4. Juan recibe el mensaje y lo descifra usando su propia clave privada (únicamente de su conocimiento)[1].

Estos sistemas de cifrado superan dos de los problemas inherentes a los de clave secreta, ambos relacionados con la gestión de claves. Primero, no se necesita un canal seguro para enviar una clave, ya que

esta es pública y podrá ser utilizada por todos aquellos que deseen cifrar información para determinadas personas. Segundo, si se tiene una comunidad de n interlocutores, el número máximo de claves que se necesita es de 2∗n frente a las n∗(n-1)/2 que se necesitaban en los criptosistemas simétricos. Además, cada usuario sólo debe recordar y proteger una sola clave[1].

Un elemento importante a considerar en los sistemas asimétricos es que al cifrar con la clave pública no se garantiza la identificación del emisor. Sin embargo, este problema se resuelve, ya que estos criptosistemas ofrecen la posibilidad de intercambiar el papel de las claves. En este caso, la clave privada puede usarse para cifrar, sabiendo que el criptograma correspondiente es descifrable mediante la clave pública, garantizando así la autenticidad del emisor. El protocolo criptográfico asociado a la autenticación del remitente sería el siguiente:

1. Alicia desea enviar un mensaje a Juan de forma que este pueda estar seguro de quién procede, para ello usará su propia clave privada (que solo es conocida por ella) para cifrar el mensaje.

2. Alicia envía el mensaje cifrado a Juan.

3. Juan recibe el mensaje y lo descifra usando la clave pública de Alicia (que es del conocimiento de todos)[1].

Si un mensaje construido según el protocolo anterior es interceptado por personas no autorizadas podrán obtener la información, ya que puede ser fácilmente descifrado con la clave pública del emisor, por lo que realizar este tipo de cifrado no es una alternativa recomendada. Con la intención de asegurar los servicios de confidencialidad y autenticación al mismo tiempo, existen los mecanismos de firma digital propuestos por la criptografía de clave pública, que serán analizados más adelante en este capítulo[1].

1.2.3. Sistemas de cifrado híbrido

Los sistemas híbridos surgen a partir de la combinación de mecanismos de cifrado simétricos y asimétricos. Estos sistemas se basan en la utilización de una clave de sesión, que no es más que una clave binaria, usada solo en el período de duración de la comunicación. Utilizan la velocidad de cifrado que

ofrecen los mecanismos simétricos para grandes volúmenes de información y la seguridad que propician los mecanismos de cifrado asimétricos para llevar a cabo una comunicación segura por canales inseguros[7].

Procedimiento de cifrado a través de criptosistemas híbridos.

1- Alicia y Juan tienen sus pares de clave, una clave privada que solo ha de conocer el propietario de la misma y una clave pública que está disponible para todos los usuarios.

2- Alicia escribe un mensaje a Juan. Lo cifra con el sistema de criptografía de clave simétrica. La clave que utiliza el algoritmo simétrico es una clave de sesión que se genera aleatoriamente, que puede ser del conocimiento de Alicia o invisible a ella.

3- Para enviar o almacenar la clave de sesión de forma segura, esta es cifrada con la clave pública de Juan, utilizando mecanismos criptográficos de clave asimétrica.

4- Juan recibe el mensaje cifrado y la clave de sesión, la cual se encuentra cifrada con su clave pública. Para obtener la información contenida en el mensaje, Juan utiliza su clave privada para descifrar la clave de sesión, y una vez que haya obtenido la clave de sesión, ya puede descifrar el mensaje [7].

1.2.4. Sistemas de cifrado irreversibles

Los sistemas irreversibles están construidos a partir de algoritmos de cifrado que no realizan el proceso inverso, siendo utilizados únicamente cuando no es necesario recuperar el mensaje en claro. Un ejemplo típico se produce cuando el mensaje en claro es una contraseña o clave de autenticación que solo es conocido por una persona (o por un sistema). Estas contraseñas se almacenan cifradas usando mecanismos irreversibles. Así, cuando una usuario accede al sistema, su identidad quedará probada si, al serle requerida la contraseña, su código cifrado coincide con el almacenado. El almacenar las contraseñas cifradas provee al sistema una gran seguridad, ya que a partir de ellas no se pueden obtener las contraseñas originales [1].

1.3. Gestión de claves

Las claves constituyen un elemento fundamental para que un algoritmo criptográfico sea seguro. Si las claves son débiles entonces el sistema de cifrado también lo será. Algunos aspectos a considerar para generar las claves son:

Distribución de claves

El problema central de los sistemas de gestión de claves radica en los procedimientos para la distribución de las claves, ya que debe efectuarse antes de la comunicación, por lo que es muy importante tener en cuenta los tipos de ataques que lo amenazan y la arquitectura del sistema. Normalmente, es necesario que la distribución de claves se realice sobre la misma red de comunicación donde se está transmitiendo la información a proteger[8].

Para llevar a cabo la distribución de claves se utilizan protocolos, que no son más que secuencias de pasos de comunicación (transferencia de mensajes) y pasos de computación. La mayoría de las propiedades de estos protocolos dependen de la estructura de los mensajes intercambiados y no de los algoritmos criptográficos. Es por ello, que sus debilidades provienen normalmente de errores cometidos en los niveles más altos del diseño [8].

Almacenamiento de claves

Existen diversas maneras de almacenar las claves, si son pequeñas, la solución más sencilla es su retención en la memoria del usuario. En caso de que las claves sean de gran longitud y difíciles de recordar, una alternativa consiste en almacenarlas en una tarjeta de banda magnética o en tarjetas inteligentes destinadas a este fin. También pueden ser almacenadas en el disco duro de la computadora del usuario, siendo peligroso porque alguien podría acceder a ellas. Para evitarlo las claves se pueden almacenar encriptadas [8].

Tiempo de vida de las claves

Una clave nunca debe usarse por tiempo indefinido por las siguientes razones:

- La probabilidad de que una clave se comprometa aumenta en dependencia de su tiempo de vida (la pérdida de una clave por medios no criptoanalíticos se denomina compromiso).

- Cuanto más tiempo de vida tenga la clave mayor será el daño si se compromete, ya que toda la información protegida con esa clave queda al descubierto.
- Es más fácil realizar criptoanálisis cuando se ha cifrado mucha información usando la misma clave [8].

Los usuarios suelen no cambiar regularmente sus claves, con lo que una solución de compromiso podría ser la actualización automática de claves. Un elemento a considerar es que las claves caducadas deben ser destruidas con la mayor seguridad, de modo que no caigan en manos de adversarios, ya que podrían leer los mensajes que fueron cifrados con dicha clave. En función del dispositivo empleado para su creación, deberá buscarse la forma de que se vuelvan irrecuperables[8].

1.4. Servicios de seguridad

Los servicios de seguridad contrarrestan los ataques a la seguridad, haciendo uso de uno o más mecanismos y políticas de seguridad. También se consideran atributos deseables para que un sistema pueda considerarse seguro. Los principales servicios de seguridad según[9] son:

- **Autenticación**: requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa. Se distinguen dos tipos: de entidad, que asegura la identidad de las entidades participantes en la comunicación, mediante biométrica (huellas dactilares, identificación de iris, etc.), tarjetas de banda magnética, contraseñas, o procedimientos similares; y de origen de información, que asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo más utilizado.
- **Confidencialidad**: requiere que la información sea accesible únicamente por las entidades autorizadas. La confidencialidad de datos se aplica a todos los datos intercambiados por las entidades autorizadas o a segmentos seleccionados de los datos, por ejemplo a través del cifrado.
- **Integridad**: requiere que la información solo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos.

La integridad asegura que los datos recibidos no han sido modificados, por ejemplo mediante un hash criptográfico con firma digital.

- **No repudio**: ofrece protección a un usuario frente a otro usuario que niegue la realización de cierta comunicación. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje. Las firmas digitales constituyen el mecanismo más empleado para este fin.
- **Control de acceso**: requiere que el acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etc.) sea controlado y limitado por el sistema destino, por ejemplo mediante el uso de contraseñas.
- **Disponibilidad**: requiere que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando los necesiten.

1.4.1. Aplicación de la criptografía moderna a los servicios de seguridad

1.4.1.1. Cifrado

La seguridad de la información es un elemento diferenciador y generador de confianza para las empresas y sus clientes. La mayoría suelen considerar que los datos que radican en dispositivos de almacenamiento internos como bases de datos o servidores, que no se mueven fuera del área de seguridad se encuentran "suficientemente seguros", así que ¿por qué preocuparse? Sin embargo, si algún atacante viola las políticas y el perímetro de seguridad tendrá acceso a toda la información que reside en los almacenes de datos, que por lo general contienen información confidencial de los clientes, empleados y sobre el funcionamiento de la empresa.

Además, un elemento de especial interés a considerar, es que el mayor activo de una empresa son sus empleados y a la vez su mayor vulnerabilidad, ya que al tener acceso a la información pueden ponerla en manos de personas no autorizadas, ya sea de forma intencional o al cometer errores como que sus contraseñas en ocasiones sean de dominio casi público y no se cambien con la frecuencia necesaria. Más preocupante aún

es que el enemigo sea el administrador de la red. Otra de las causas más comunes de divulgación no autorizada de información es la pérdida de dispositivos de almacenamiento portátiles, ya sea accidentalmente o por ser víctimas de un robo.

Luego de un análisis sobre los riesgos que traen para las empresas no explorar eficazmente las vulnerabilidades de almacenar la información y considerando que las amenazas contra la seguridad de la información cada vez son más generalizadas, se hace necesario agregar medidas de protección que garanticen la privacidad de la información.

El uso de mecanismos de cifrado que transformen la información para que solo puedan acceder a ella las personas autorizadas, es una de las técnicas más usadas en la actualidad. Su objetivo fundamental es garantizar la confidencialidad de los documentos incluso cuando alguien pueda sustraer ficheros que posean información cifrada. Las técnicas de cifrado, además de garantizar la confidencialidad, garantizan colateralmente la integridad, debido a que si el documento no es accesible para usuarios no autorizados tampoco es modificable.

El cifrado es una de las muchas salvaguardas que se deben considerar, ofrece una protección muy poderosa contra los actos intencionales y no intencionales. Es importante tener en cuenta que el cifrado no debe ser el único medio aplicado para proteger la información y el coste de la protección en ningún caso puede superar el valor de la propia información que se desea proteger.

1.4.1.2. Firma Digital

La firma manuscrita es todavía la forma más utilizada y “confiable” para relacionar un documento con una persona en particular de manera legal. Sin embargo, este método posee diversas imperfecciones como la posibilidad de falsificación. Otra limitación que presenta se debe a la necesidad de contar con la presencia física de las personas involucradas y la de un notario que garantice su validez, lo cual hace lenta y costosa una transacción entre empresas que se encuentren geográficamente distantes. Precisamente, como solución a estos problemas nace una nueva tecnología denominada firma digital.

La firma digital es una de las aplicaciones de la criptografía moderna y es utilizada para establecer la autenticidad e integridad de mensajes y documentos electrónicos. La verificación de la firma digital permite determinar cuando un mensaje o documento ha sido alterado. Además, tiene la propiedad de que solo puede ser producida de manera correcta por una entidad, y ser verificada por cualquiera que reciba el mensaje o documento firmado digitalmente [10].

Asimismo, si se quiere establecer evidencia de que la información fue firmada en un instante de tiempo determinado, a la firma digital de los documentos, se le puede añadir una indicación del momento en que se realizó, conocido como "sello de tiempo". Es importante destacar que un documento electrónico firmado digitalmente puede ser público, porque integridad y autenticidad no implican necesariamente confidencialidad.

La firma digital involucra dos acciones: la acción de firmar y la acción de verificación de la firma. A continuación se explican estos procedimientos.

Generación de la firma digital: se le aplica una función resumen al documento que se quiere firmar y se obtiene una secuencia de bits que identifica de manera unívoca al documento. El código obtenido se cifra con la clave privada del emisor del documento. Finalmente, se envía el documento y el resumen del mensaje cifrado que representa la firma digital. De esta forma, el signatario protege la integridad del documento, pues le incorpora una marca que solo él es capaz de realizar[7].

Verificación de la firma: el receptor separa el documento de la firma digital, calcula el HASH del documento y descifra utilizando la clave pública del emisor la firma digital enviada. Si el resultado que se obtiene por los dos caminos es el mismo, significa que el documento conserva su autenticidad e integridad[7].

1.5. Portafirmas Digitales

En la administración electrónica de documentos, es cada vez más frecuente la implantación de la firma electrónica para la tramitación de documentos mediante sistemas de información, así como en gestiones de índole interna.

Debido a la diversidad de sistemas de información que gestionan y tramitan los diferentes procedimientos, el coste de implantar la firma electrónica en cada sistema de información, tanto en tiempo como en complejidad es extremadamente elevado, ya que cada sistema de información está basado en tecnologías y arquitecturas diferentes. Esto provocó el desarrollo de un aplicativo que gestionase la firma electrónica de documentos electrónicos creados por distintos medios y sistemas de información de manera centralizada.

Los portafirmas digitales son herramientas destinadas a facilitar a los órganos y unidades administrativas el uso de la firma digital de documentos, procedentes de diferentes sistemas de información independientes, con la consiguiente agilización de la actividad administrativa. Se trata de herramientas de usuario final que utilizan y proveen servicios de autenticación y firma digital que tienen – *siempre que las normativas jurídicas lo estipulen* – el mismo valor que la firma manuscrita [11].

A través de la firma digital, los portafirmas digitales, incluyen en los documentos un código seguro de verificación generado electrónicamente, que permite constatar su integridad y autenticidad. Los documentos emitidos por órganos y unidades, firmados con herramientas de este tipo pudieran gozar de la validez y eficacia de documentos originales.

Los objetivos específicos de los portafirmas digitales son principalmente:

- Centralización en un único punto de la firma de documentos electrónicos procedentes de distintos trámites soportados por diferentes aplicaciones.
- Homogeneización y estandarización de la práctica de la firma electrónica.
- Reducción del soporte físico (papel) de los documentos y del movimiento a través de organismos, contribuyendo a la sostenibilidad medioambiental de la actividad administrativa.
- Agilización de la actividad administrativa de los trámites.
- Posibilidad de firmar documentos en cualquier lugar.
- Implementación de distintos tipos de firma.

- Capacidad para recuperar el documento original firmado electrónicamente para poder constatar la integridad y autenticidad de cualquier copia emitida [12].

A continuación, se expondrán algunas características de portafirmas utilizados en el ámbito internacional:

1.5.1. Portafirmas, Universidad Murcia

Es la herramienta corporativa de firma electrónica de documentos en la Universidad de Murcia, que permite a sus usuarios firmar, en un único paso, todos sus documentos pendientes, así como gestionarlos e imprimir copias auténticas de los mismos. Entre las características que soporta la herramienta se pueden destacar:

- Autenticación de usuarios contra el directorio.
- Generación de solicitudes de firma con múltiples documentos desde un usuario solicitante.
- Gestión de preferencias de usuario (notificaciones, autorizaciones, revisores y flujos).
- Envío de solicitudes firmadas a otros usuarios para su consulta.
- Carga masiva de documentos en la generación de solicitudes de firma [13] .

1.5.2. Porta@firmas, Universidad de Sevilla

Porta@firma es una herramienta ofrecida por la Junta de Andalucía e incorporada a la plataforma de tramitación electrónica de la Universidad de Sevilla, con la intención de realizar la firma electrónica de documentos procedentes de diferentes sistemas de información independientes. Esta aplicación web utiliza los servicios proporcionados por la plataforma @firma de autenticación, firma electrónica, seguimiento de las firmas realizadas y verificación de las mismas. El modo de autenticación definido por este sistema es la lectura de los datos del certificado digital, el cual puede ser escogido si el usuario posee más de uno. Las principales características que incorpora la herramienta Porta@firma son:

- Posibilidad de firma documentos en bloque (hasta 25 documentos).
- Posibilidad de firmar documentos desde cualquier ubicación.
- Gestión de la firma de documentos. Esta función consiste en una interfaz web bajo la metáfora de escritorio de firma dividida en tres partes: documentos pendientes de firma, documentos pendientes de la firma de un firmante anterior (firma en cascada), documentos firmados por el usuario y documentos enviados de nuevo al emisor. Se requiere autenticación previa del usuario mediante certificado digital.
- Verificación de firmas de documentos. Esta función consiste en una interfaz web que, a partir del código seguro de verificación del documento firmado, permite recuperar y mostrar el original para su cotejo.
- Avisos de correo al firmante informándole si tiene algún documento pendiente de firma [12].

1.5.3. Portafirmas, Viafirma Inbox

Viafirma Inbox es una aplicación web que sigue el prototipo de un cliente de correo, el cual permite la gestión de firma de documentos electrónicos pendientes de firmar, así como la visualización. Organiza la agenda de firma gracias a la notificación y planificación de la caducidad de los documentos a firmar. Sus principales características son:

- Servicios de verificación de copias auténticas mediante el uso de la Firma Digital. Permite firmar cualquier tipo de documentos.
- Posibilidad de firmar documentos desde cualquier ubicación.
- Facilita la auditoría del sistema.
- Permite la búsqueda de documentos.
- Posibilita el envío de peticiones de firmado a direcciones de correo electrónico de usuarios que no se encuentran en el sistema, realizando el registro en el momento del acceso del mismo.

- Permite la firma desde dispositivos móviles.
- Sistema multiplataforma [14].

Luego de realizar un análisis sobre algunos de los portafirmas digitales utilizados en la actualidad se concluye que no tienen integrado una solución para cifrar documentos, únicamente se ocupan de ofrecer a los usuarios la posibilidad de firmar digitalmente los documentos, lo que puede constituir una debilidad en la seguridad de la información de dichos sistemas.

Lo anteriormente expuesto evidencia lo novedoso de la solución propuesta, ya que los sistemas analizados no cuentan con las funcionalidades de cifrado que se pretenden integrar al Portafirmas Digit@l para garantizar la confidencialidad de la información.

Análisis del capítulo

- Se expusieron los principales puntos de interés relacionados con la criptografía moderna, explicando los términos básicos que la hacen comprensible.
- El estudio realizado sobre los mecanismos criptográficos permitió identificar que los mecanismos híbridos son los más eficientes y seguros para cifrar información, ya que los mecanismos simétricos son muy rápidos para cifrar grandes volúmenes de datos pero no son seguros en cuestiones de transmisión de claves y los mecanismos asimétricos ofrecen seguridad en este aspecto pero consumen muchos recursos computacionalmente en el cifrado de mucha información.
- El estudio realizado sobre algunos portafirmas digitales que se utilizan en el mundo permitió identificar que el cifrado de documentos es un aspecto no incluido, por lo que constituye una novedad incorporarlo como parte de las funcionalidades de la herramienta Portafirmas Digit@l.

Capítulo 2

El contexto del sistema. Especificación de requisitos

El actual capítulo presenta una visión general de la captura de los requisitos, definida por Jacobson, Booch y Rumbaugh en su libro El Proceso Unificado de Desarrollo de Software como: *"el proceso de averiguar, normalmente, en circunstancias difíciles, lo que se debe construir"*[15], realizándose a través de cuatro fases fundamentales: enumeración de requisitos candidatos, comprensión del contexto del sistema, captura de los requisitos funcionales y no funcionales, así como la especificación de éstos como casos de uso del sistema.

2.1. Metodología de desarrollo: RUP

RUP como metodología es un proceso de desarrollo de software que define quién está haciendo qué, cuándo y cómo alcanzar un determinado objetivo. Se caracteriza por ser iterativo e incremental, estar centrado en la arquitectura y guiado por casos de uso. Es adaptable al contexto y a las necesidades de cada organización con el propósito de obtener un producto de software con calidad.

Se seleccionó la metodología RUP para dirigir el proceso de desarrollo de la solución propuesta teniendo en cuenta lo antes expuesto y que permitirá mantener un proceso homogéneo entre el desarrollo de la solución de cifrado de documentos y el Portafirmas Digit@l, pues RUP es la metodología usada para guiar sus procesos.

2.2. Lenguaje de programación: Java

Java es un lenguaje de programación que su robustez lo han convertido en uno de los más usados en ámbitos de la informática. Ofrece un ambiente de programación seguro y posee independencia de la

plataforma, por lo que programas escritos en el lenguaje Java pueden ejecutarse igualmente en cualquier tipo de hardware y/o software.

Java ofrece funciones criptográficas de propósito general, denominadas Arquitectura Criptográfica de Java (JCA) y Extension Criptográfica de Java (JCE). JCA permite la generación de firmas digitales y resúmenes de mensajes y JCE proporciona implementaciones para cifrado y descifrado de datos, algoritmos MAC(Message Authentication Code), generación y acuerdo de claves.

Por lo antes expuesto se propone para el desarrollo del módulo de cifrado de documentos el lenguaje de programación Java. Además, para lograr una mejor integración con el Portafirmas Digit@l, ya que para su implementación se definió el lenguaje Java.

2.3. Lenguaje de modelado: UML

Se seleccionó el lenguaje UML para modelar los artefactos generados en el proceso de desarrollo de software, ya que el uso de lenguajes visuales facilitan el entendimiento por parte del equipo de desarrollo sobre el sistema que se modela. Además, proporciona una forma estándar de modelado, cubriendo todo lo relacionado a los procesos del negocio.

2.4. Herramienta CASE: Visual Paradigm

Visual Paradigm es una herramienta que soporta el ciclo de vida completo del desarrollo de software: análisis y diseño, construcción, pruebas y despliegue. Algunas de sus características son:

- Ofrece un lenguaje estándar común a todo el equipo de desarrollo.
- Su licencia es gratuita y comercial.
- Capacidades de ingeniería directa e inversa.
- Soporte de UML.

Teniendo en cuenta las elementos anteriormente expuestos se empleará la herramienta Visual Paradigm para realizar la construcción de los artefactos generados en el proceso de desarrollo de la presente solución.

2.5. Requisitos candidatos

"Durante la vida del sistema, los clientes, usuarios, analistas y desarrolladores aparecen con muchas buenas ideas que podrían convertirse en verdaderos requisitos. Mantenemos una lista de estas ideas, que consideramos como un conjunto de requisitos candidatos que podemos decidir implementar en una versión futura del sistema"[15].

Con el objetivo de incrementar la seguridad de la información contenida en documentos que se encuentran en el repositorio de contenidos del Portafirmas Digit@l, se propone desarrollar una solución que se caracterice por:

- **Cifrado y descifrado de documentos**: capacidad de la solución para aplicar técnicas de cifrado y descifrado de documentos.
- **Cifrado simétrico de documentos**: capacidad de la solución de cifrar los documentos a través de algoritmos de cifrado simétrico.
- **Intercambio seguro de claves**: capacidad de la solución que garantiza la transmisión de las claves por canales inseguros sin pérdida de su seguridad.
- **Soporte para la actualización de claves**: capacidad de la solución que garantiza el acceso de los usuarios a la información contenida en documentos cifrados para ellos, aun cuando su clave se modifique.

2.6. El contexto del sistema. Modelo de Dominio

Los artefactos que propone la metodología RUP para comprender el contexto del sistema son el modelo del dominio y el modelo del negocio. Para realizar el modelo del negocio es necesario conocer como se realizan cada uno de los procesos y estados del negocio que se quiere automatizar, así como las competencias requeridas en cada proceso: sus trabajadores, sus responsabilidades, y las operaciones que llevan a cabo.

El modelo del negocio actual presenta un bajo nivel de estructuración, siendo difícil identificar las personas que participan en las distintas actividades en cada uno de los procesos, por lo que se decide realizar el modelo de dominio que RUP propone para estos casos.

"Un modelo de dominio captura los tipos más importantes de objetos en el contexto del sistema. Los objetos del dominio representan las "cosas" que existen o los eventos que suceden en el entorno en el que trabaja el sistema"[15].

2.6.1. Diagrama de clases del modelo de dominio

En la siguiente figura, se presenta el modelo del dominio mediante un diagrama UML. Su propósito fundamental es contribuir a la comprensión del contexto del sistema a través de los objetos identificados, así como de los eventos que suceden en el entorno en que se desarrolla tal problema.

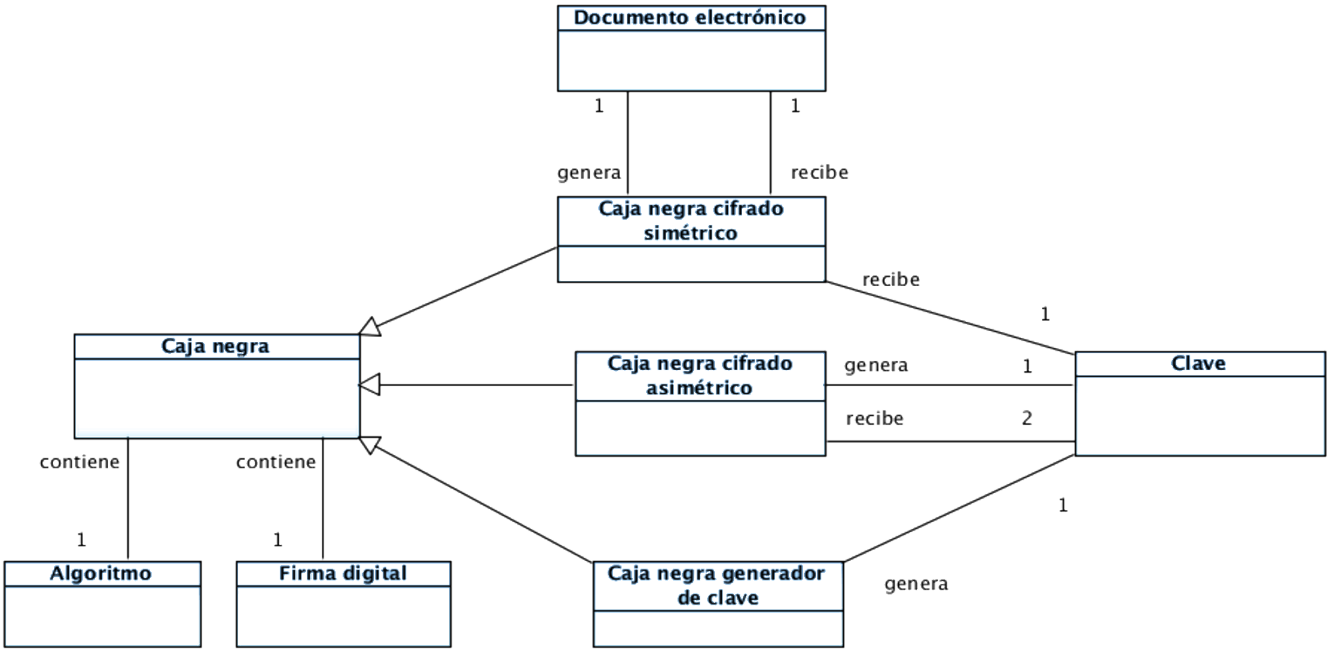

Figura 2.1: Modelo de dominio

2.6.1.1. Descripción de las clases del modelo de dominio

- **Documento electrónico**: toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior[16].
- **Clave**: código de signos convenidos para la transmisión de mensajes secretos o privados[2].
- **Algoritmo**: conjunto ordenado y finito de operaciones que permite hallar la solución de un problema[2].
- **Firma Digital**: son secuencias de caracteres que, tras la aplicación de unos complejos procedimientos algorítmicos y claves (una larga cadena de dígitos análogos a una contraseña), se pueden emplear para verificar la integridad de un documento de archivo o la autenticidad de la identidad del remitente de un documento de archivo[17].

- **Caja negra**: de manera general, una caja negra se compone de un algoritmo que recibe un conjunto de entradas (conjunto que puede ser nulo) y las transforma en una o más salidas. Incluye además, un fichero con la firma digital del algoritmo emitida por su proveedor, con el objetivo de garantizar su autenticidad e integridad.

  Las cajas negras que participan en el contexto del sistema son:

- **Caja negra generador de clave**: contiene un algoritmo que no recibe valores de entrada y genera aleatoriamente claves de sesión, que serán utilizadas como entrada por los algoritmos simétricos, con el propósito de cifrar o descifrar documentos electrónicos según sea el caso.

- **Caja negra cifrado simétrico**: contiene un algoritmo de cifrado simétrico que recibe como entrada un documento electrónico y una clave de sesión, generando como salida un documento electrónico.

- **Caja negra cifrado asimétrico**: contiene un algoritmo de cifrado asimétrico que recibe como entrada dos claves, una de las cuales siempre es la clave de sesión.

  - Si lo que se desea es cifrar la clave de sesión, entonces el algoritmo debe recibir como entrada la clave de sesión y la clave pública del usuario que podrá descifrarlo, generando como salida la clave de sesión cifrada.
  - Si lo que se desea es descifrar la clave de sesión, entonces el algoritmo debe recibir como entrada la clave de sesión cifrada y la clave privada del usuario que desea descifrarla, generando como salida la clave de sesión descifrada.

2.7. Captura de requisitos

2.7.1. Requerimientos funcionales

Teniendo en cuenta que *"los requerimientos funcionales son declaraciones de los servicios que debe proporcionar el sistema, de la manera en que éste debe reaccionar a entradas particulares y de cómo se*

debe comportar en situaciones particulares"[18], se determinó que la solución debe contar con las siguientes funcionalidades.

- **R1. Cifrar documento local:** surge a partir de la necesidad que tiene el cliente de compartir con un determinado conjunto de usuarios, información confidencial plasmada en documentos que se encuentran en el disco duro de su ordenador. Para ello se cifrará el documento en su computadora y luego será incorporado al repositorio de contenidos del Portafirmas Digit@l.
- **R2. Cifrar documento en el servidor:** una vez que un usuario identifique que en el repositorio de contenidos del Portafirmas Digit@l existen documentos con información confidencial, expuesta a personas no autorizadas como los administradores del sistema, procede a cifrar el documento, reeemplazando el original.
- **R3. Descifrar documento local:** surge a partir de la necesidad que tiene el usuario, de obtener para consumo propio determinada información contenida en un documento cifrado que reside en el repositorio de contenidos del Portafirmas Digit@l.
- **R4. Descifrar documento en el servidor:** cuando la información de un documento cifrado deja de ser confidencial, se procede a descifrar el documento en el servidor, reemplazando la versión cifrada por el documento original, haciendo pública la información para todos los usuarios.
- **R5. Listar documentos cifrados:** surge a partir de la necesidad que tiene el usuario de saber que documentos han sido cifrados para él o por él.

2.7.2. Requerimientos no funcionales

"Los requerimientos no funcionales, como su nombre sugiere, son aquellos requerimientos que no se refieren directamente a las funciones específicas que proporciona el sistema, sino a las propiedades emergentes de éste como la fiabilidad, el tiempo de respuesta y la capacidad de almacenamiento " [18].

Los requerimientos no funcionales son clasificados en diferentes categorías. A continuación se muestran los que se definieron para la presente solución.

- **Usabilidad:**
  - **RNF 1. Tipo de aplicación**: la solución debe ser una aplicación de escritorio.
  - **RNF 2. Finalidad**: la aplicación debe garantizar la confidencialidad de la información contenida en documentos que son o serán incorporados al repositorio de contenidos del Portafirmas Digit@l.
- **Restricciones de diseño:**
  - **RNF 3. Lenguajes de Programación:** el lenguaje de programación empleado para desarrollar la aplicación debe ser Java.
- **Soporte:**
  - **RNF 4. Estándar de codificación:** se debe emplear el lenguaje de codificación de Java.
- **Portabilidad**
  - **RNF 5:** el sistema debe ser multiplataforma.

2.8. Especificación de requisitos como casos de uso

2.8.1. Casos de uso del sistema

"Cada forma en que los actores usan el sistema se representa con un caso de uso. Los casos de uso son "fragmentos"de funcionalidad que el sistema ofrece para aportar un resultado de valor para sus actores. De manera más precisa, un caso de uso especifica una secuencia de acciones que el sistema puede llevar a cabo interactuando con sus actores, incluyendo alternativas dentro de la secuencia" [15].

A partir de los requisitos identificados, se propone el siguiente diagrama de casos de uso, que contiene los actores, casos de uso (que responden a 1 o más requisitos) y las relaciones que se establecen entre éstos, o sea, la forma en que los actores usan el sistema.

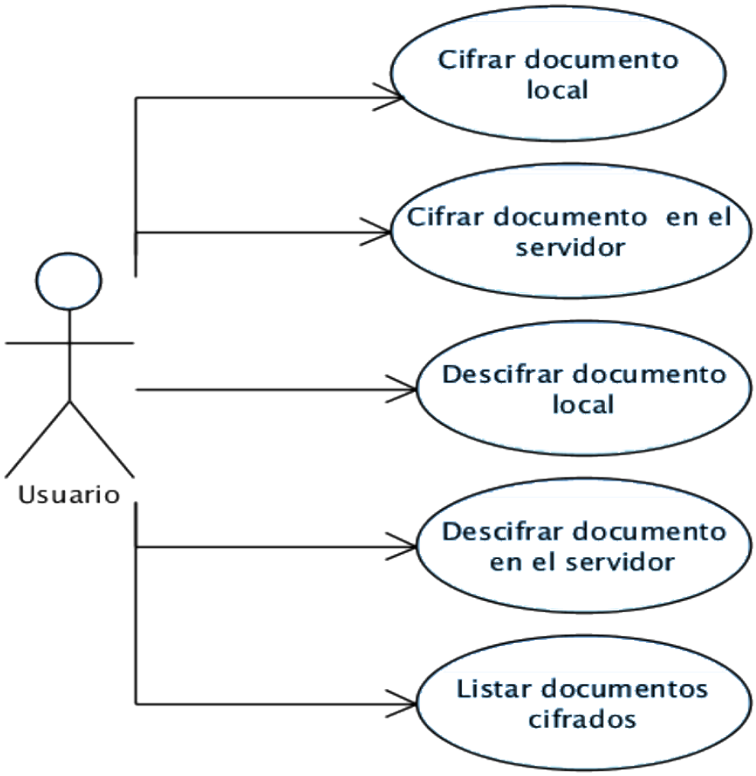

Figura 2.2: Diagrama de casos de uso del sistema

2.8.2. Definición de actores del sistema

"Un actor juega un papel por cada caso de uso con el que colabora. Cada vez que un usuario en concreto (un humano u otro sistema) interactúa con el sistema, la instancia correspondiente del actor está desarrollando su papel. Una instancia de un actor es por tanto un usuario concreto que interactúa con el sistema" [15] .

Actor	Justificación
Usuario	Es la persona con necesidad de cifrar o descifrar documentos.

Tabla 2.1: Definición de actores del sistema

2.8.3. Descripciones textuales de los casos de uso del sistema

Caso de uso	**Cifrar documento local**
Actor	Usuario
Resumen	El caso de uso inicia cuando el usuario selecciona (en la barra de herramientas del Portafirmas Digit@l) la opción cifrar documentos local y finaliza cuando el documento es cifrado e incorporado al repositorio de contenidos de dicho sistema.
Prioridad	Crítico
Complejidad	Media
Referencias	R1
Precondiciones	
Poscondiciones	
Flujo de eventos	
Actor	**Sistema**
Continúa en la próxima página	

1. Selecciona (en la barra de herramientas del Portafirmas Digit@l) la opción cifrar documento local.	2. Muestra en una nueva ventana un formulario para que el usuario seleccione o especifique las siguientes opciones: ▪ Cajas negras de generación aleatoria de claves de sesión. ▪ Cajas negras de cifrado simétrico. ▪ Cajas negras de cifrado asimétrico. ▪ Listado de usuarios (registrados en el sistema). ▪ Botón examinar (le permitirá al usuario navegar por el sistema de ficheros de su computadora para buscar el documento que desea cifrar).
3. Selecciona las opciones requeridas para cifrar el documento y presiona el botón cifrar.	4. Verifica que todas las opciones fueron seleccionadas correctamente.
	5. Genera la clave de sesión.
	6. Cifra el documento y las claves de sesión.
	7. Envía el documento cifrado y las claves de sesión cifradas al repositorio de contenidos. Finaliza el caso de uso.
Flujos alternos	
Actor	**Sistema**
	4.1 Identifica las opciones que no fueron seleccionadas y muestra un mensaje de error.

Continúa en la próxima página

	4.2 Regresa al paso 2 del flujo normal de eventos.
	7.1 Muestra un mensaje de error en caso de no existir conexión con el repositorio de contenidos.

Tabla 2.2: Descripción: CU Cifrar documento local.

Caso de uso	**Cifrar documento en el servidor**
Actor	Usuario
Resumen	El caso de uso inicia cuando el usuario selecciona (en la barra de herramientas del Portafirmas Digit@l) la opción: cifrar documentos en el servidor y finaliza cuando el documento es cifrado.
Prioridad	Crítico
Complejidad	Media
Referencias	R2
Precondiciones	
Poscondiciones	
Flujo de eventos	
Actor	**Sistema**
Continúa en la próxima página	

1. Selecciona (en la barra de herramientas del Portafirmas Digit@l) la opción cifrar documento local.	2. Muestra en una nueva ventana un formulario para que el usuario seleccione o especifique las siguientes opciones: ▪ Cajas negras de generación aleatoria de claves de sesión. ▪ Cajas negras de cifrado simétrico. ▪ Cajas negras de cifrado asimétrico. ▪ Listado de usuarios (registrados en el sistema). ▪ Botón examinar (le permitirá al usuario navegar por el sistema de ficheros de su computadora para buscar el documento que desea cifrar).
3. Selecciona las opciones requeridas para cifrar el documento y presiona el botón cifrar.	4. Verifica que todas las opciones fueron seleccionadas correctamente.
	5. Envía los datos al servidor para que realice el proceso de cifrado. Finaliza el caso de uso.
Flujos alternos	
Actor	**Sistema**
	4.1 Identifica las opciones que no fueron seleccionadas y muestra un mensaje de error.
	4.2 Regresa al paso 2 del flujo normal de eventos.
	5.1 Muestra un mensaje de error en caso de no existir conexión con el repositorio de contenidos.

Continúa en la próxima página

Tabla 2.3: Descripción: CU Cifrar documento en el servidor.

Caso de uso	**Descifrar documento local**
Actor	Usuario
Resumen	El caso de uso inicia cuando el usuario selecciona (en la barra de herramientas del Portafirmas Digit@l) la opción descifrar documento local y finaliza cuando el documento es descifrado.
Prioridad	Crítico
Complejidad	Media
Referencias	R3
Precondiciones	
Poscondiciones	
Flujo de eventos	
Actor	**Sistema**
1. Selecciona (en la barra de herramientas del Portafirmas Digit@l) la opción: descifrar documento local.	2. Muestra en una nueva ventana un listado de los documentos cifrados que el usuario puede descifrar.
3.Selecciona el documento cifrado.	4. Solicita la clave privada del usuario y la ubicación del directorio en su computadora, en el cual se guardará el documento descifrado.
	5. Descifra el documento. Finaliza el caso de uso.
Flujos alternos	
Actor	**Sistema**

Continúa en la próxima página

	2.1 Muestra un mensaje informando que el usuario no tiene documentos para descifrar. Finaliza el caso de uso

Tabla 2.4: Descripción: CU Descifrar documento local.

Caso de uso	**Descifrar documento en el servidor.**
Actor	Usuario
Resumen	El caso de uso inicia cuando el usuario selecciona (en la barra de herramientas del Portafirmas Digit@l) la opción descifrar documento en el servidor y finaliza cuando el/los documentos son descifrados.
Prioridad	Crítico
Complejidad	Media
Referencias	R4
Precondiciones	
Poscondiciones	
Flujo de eventos	
Actor	**Sistema**
1. Selecciona (en la barra de herramientas del Portafirmas Digit@l) la opción descifrar documento en el servidor.	2. Muestra en una nueva ventana un listado con todos los documentos que fueron cifrados por el usuario.
3.Selecciona el o los documentos que desea descifrar y presiona el botón aceptar.	4. Solicita la clave privada del usuario.
5. Especifica la ubicación de su clave privada y oprime el botón descifrar.	6. Envía los datos al servidor para que realice el proceso de descifrado. Finaliza el caso de uso.
Continúa en la próxima página	

Flujos alternos	
Actor	**Sistema**
	2.a.1 Muestra un mensaje informando que el usuario no tiene documentos para descifrar.
	6.1 Muestra un mensaje de error en caso de no existir conexión con el servidor (en el cual se encuentra el repositorio de contenidos).

Tabla 2.5: Descripción: CU Descifrar documento en el servidor.

Caso de uso	**Listar documentos cifrados**
Actor	Usuario
Resumen	El caso de uso inicia cuando el usuario selecciona (en la barra de herramientas del Portafirmas Digit@l) la opción: listar los documentos cifrados y finaliza cuando se muestra el listado.
Prioridad	Auxiliar
Complejidad	Baja
Referencias	R5
Precondiciones	
Poscondiciones	
Flujo de eventos	
Actor	**Sistema**
Continúa en la próxima página	

1. Selecciona (en la barra de herramientas del Portafirmas Digit@l) la opción listar documentos cifrados.	2. Muestra en una nueva ventana un listado con todos los documentos cifrados. Finaliza el caso de uso.
Flujos alternos	
2.a No hay documentos cifrados	
	2.1 Muestra un mensaje especificando que no hay documentos cifrados en el repositorio de contenidos del portafirmas Digit@l.

Tabla 2.6: Descripción: CU Listar documentos cifrados.

2.8.4. Prototipo de interfaz de usuario

Los prototipos de interfaz de usuario permiten comprender y especificar las interacciones entre actores humanos y el sistema durante la captura de requisitos. No sólo ayudan a desarrollar una interfaz gráfica mejor, sino también a comprender mejor los casos de uso [15].

Para ver los prototipos de interfaz ver Anexo A de la versión extendida de este documento.

Análisis del capítulo

En el contenido de este capítulo se describió el proceso realizado para capturar los requisitos a partir de los artefactos:

- **Modelo de dominio**: durante la concepción y la conceptualización del contexto del sistema.
- **Modelo de casos de uso**: se describe detalladamente cómo se le irá dando respuestas a los requisitos a partir de la interacción usuario-sistema.

- **Prototipos de interfaz de usuario**: ofrecen una visión inicial de como puede quedar el sistema en términos de interfaz de usuario.

Las técnicas de captura de requisitos antes expuestas permitieron identificaron las principales necesidades y funcionalidades que deberían incorporarse a la solución en general. Este resultado constituye el punto de partida para la ejecución de los próximos flujos de trabajos.

Capítulo 3

Protocolos criptográficos

"Un protocolo es el conjunto de acciones coordinadas que realizan dos o más partes o entidades con el objeto de llevar a cabo un intercambio de datos o información" [4].

En criptografía, un protocolo representa el orden en que se ejecutan los algoritmos de cifrado para resolver un problema criptográfico de forma segura, si estos pasos no son realizados de forma correcta, se puede romper la seguridad del sistema criptográfico, aunque todos los algoritmos utilizados sean totalmente seguros [19].

3.1. Roles que participan en un protocolo

En un protocolo criptográfico intervienen diferentes roles, tales como: personas, sistemas externos, entidades, entre otros. A continuación se presentan ejemplos de los roles que con más frecuencia intervienen en un protocolo criptográfico.

- **Interlocutores:** en una comunicación puede participar un único interlocutor A (p.e. encriptar un fichero), dos interlocutores A, B (p.e. en una comunicación cifrada), o incluso más de dos interlocutores [19].
- **Árbitros:** participante que actúa cuando entre las partes involucradas en la comunicación no existe confianza, por lo que tiene que ser imparcial y ambos se someten a las resoluciones del árbitro. Un tipo de árbitro son los expendores de certificados digitales, que se encargan de firmar documentos para demostrar su autenticidad [19].
- **Atacantes:** individuos que no deben formar parte del protocolo. Comúnmente son clasificados como pasivos o activos: los primeros solamente intentan acceder a los datos intercambiados sin realizar modificaciones a los datos, los segundos son más peligrosos ya que pueden ver y modificar los datos

que se intercambian en el protocolo. Si existiese un participante del protocolo que sea un atacante activo se le llama atacante mentiroso y son aún más peligrosos [19].

- **Sistemas externos:** pueden actuar como árbitros para garantizar la seguridad en la comunicación entre interlocutores que pueden encontrase geográficamente distantes. Un ejemplo de este tipo de rol pueden ser los expendedores de certificados (PKI), que generan los certificados digitales que usarán los usuarios para identificar y autentificar al resto de los usuarios en una comunicación [19].

3.2. Model checking

Model checking se ha convertido en un elemento fundamental en el diseño de sistemas distribuidos, permitiendo asegurar la correctitud del diseño lo más temprano posible. Sus dos ventajas fundamentales, comparada con otras técnicas como simulación y pruebas son:

- No es necesario construir un prototipo funcional del sistema.
- Permite verificar el sistema completo en cada traza de ejecución.

La última es muy importante porque a través de la simulación o pruebas se pueden encontrar errores pero no es posible asegurar que el sistema se comportará tal como se espera, algunos errores pueden permanecer ocultos hasta que el sistema se comience a explotar [20].

En un proceso de diseño en el cual se aplica "Model checking"se distinguen los siguientes pasos.

1. **Fase de modelado:** primeramente se identifican los requerimientos del sistema. Una vez que se conocen tales requerimientos, estos deben ser formalizados a través de propiedades en un lenguaje de especificación de propiedades. Luego, debe especificarse un modelo del sistema en un lenguaje de entrada. Además, pueden ejecutarse un conjunto de simulaciones con el objetivo de encontrar errores al modelo[20].
2. **Fase de ejecución:** se ejecuta el modelo para verificar la validez de sus propiedades[20].

3. **Fase de análisis:** si no se encuentran errores, se puede continuar probando la siguiente propiedad. En cambio, si se viola la propiedad de seguridad, entonces será necesario analizar la salida, en tal caso será necesario refinar el modelo o la propiedad y repetir el proceso [20].

3.2.1. Fase de modelado

Durante la fase de modelado se ejecutan las siguientes actividades:

- **Definición del problema**: el objetivo de esta actividad es dar una descripción general del modo de operación o funcionamiento del protocolo.
- **Definición de las variables**: se definen los tipos de datos básicos y las funciones.
- **Definición de los participantes**: se declaran los agentes que forman parte o juegan un rol específico durante la ejecución del protocolo.
- **Descripción del protocolo**: se especifica la secuencia normal de mensajes para una ejecución del protocolo.
- **Especificación de las propiedades**: se enumeran las propiedades de seguridad que el modelo debe satisfacer [20].

3.3. Protocolos criptográficos

3.3.1. Definición de los roles

En los protocolos que se describirán a continuación participan los siguientes roles :

- **Cliente:** interlocutor que inicia la comunicación (emisor), a los efectos, se trata de una instancia del Portafirmas Digit@l iniciada por un usuario.

- **Servidor:** interlocutor que recibe la solicitud de comunicación por parte del cliente (receptor), se trata del servidor donde se encuentra disponible el repositorio de contenidos del Portafirmas Digit@l.
- **Intruso:** se trata de cualquier agente que, de alguna manera interfiere en la comunicación *-pasiva o activamente-* y no es ninguno de los agentes cliente o servidor. A los efectos el intruso puede ejecutar alguna de las siguientes operaciones:
  - Escuchar e interceptar la comunicación.
  - Modificar los mensajes.
  - Generar nuevos mensajes.
  - Enviar los mensajes capturados a otra entidad.

3.3.2. Establecimiento de Conexión

3.3.2.1. Descripción del protocolo

El presente protocolo brinda una capa de abstracción entre una aplicación cliente (en este caso una instancia del Portafirmas Digit@l) y su repositorio de contenidos, en lo siguiente denominado servidor. La idea es permitir - *de manera transparente* - el cifrado de los datos intercambiados entre el cliente y el servidor estableciendo para ello sesiones y/o conexiones seguras.

Cada vez que, desde un cliente del Portafirmas Digit@l se desee ejecutar alguna de las funcionalidades identificadas, se ejecutarán - *de manera general* - como parte de este protocolo los pasos que se enuncian a continuación:

1. Se inicia automáticamente el protocolo a la vez que el usuario ejecuta alguna de las funcionalidades que provee el módulo de cifrado.
2. Como el cliente tiene conocimiento del Certificado del Servidor (CS) le exige a este último que se autentique. Para ello, le envía al servidor un mensaje generado aleatoriamente.

3. El servidor cifra el mensaje obtenido con su clave privada y se lo envía al cliente, procedimiento similar al de la firma digital.

4. El cliente verifica que ciertamente está interactuando con el servidor adecuado y en caso afirmativo se inicia la transferencia de datos entre cliente y servidor.

3.3.2.2. Requerimientos del protocolo

Bajo la premisa de que una vez ejecutado el protocolo, si se logra establecer una sesión, el intercambio de datos durante la comunicación se realizará de manera segura, se establecen los siguientes objetivos:

- Sincronizar las partes involucradas.
- Intercambio de datos para generar claves de sesión seguras.
- Negociar parámetros de sesión como son los algoritmos de cifrado a utilizar, métodos de compresión, funciones hash, tamaño de las claves, entre otros.

3.3.2.3. Propiedades de seguridad

Cuando un cliente establece una sesión con el servidor se garantizan las siguientes propiedades de seguridad:

- **Conexión privada**: los mensajes entre cliente y servidor son cifrados.
- **Autenticación cliente-servidor**: cada agente se autentica con su par de clave pública y privada.
- **La conexión es confiable**: es posible verificar la integridad de los mensajes.

3.3.2.4. Modelado del protocolo

El cliente inicia la comunicación con el servidor a través de una petición del usuario. Como parte del mensaje se envían los datos identificativos del usuario -*recordando que el usuario tiene conocimiento del*

servidor, pero este último no tiene la menor idea de con qué cliente se está comunicando-, un mensaje generado aleatoriamente cifrado con la clave pública del servidor junto con el algoritmo empleado para cifrar tal clave, una lista de suites de cifrado y otra de métodos de compresión, todo ello firmado digitalmente a nombre del usuario que está interactuando con la aplicación cliente.

Una vez que el servidor recibe tal mensaje, con los datos identificativos del usuario, procede a verificar que el usuario es realmente quien dice ser, comprobando la validez de la firma antes citada. Si esta es válida entonces el servidor firma el mensaje enviado por el cliente, selecciona la suite de cifrado que empleará durante la comunicación, el método de compresión y genera una clave aleatoria que cifrará con la clave pública del usuario, usando el mismo mecanismo de cifrado empleado por el usuario para generar la clave enviada. Finalizada esta operación el servidor envía la respuesta al cliente.

Al recibir la respuesta, el cliente verificará la validez de la firma del mensaje enviado inicialmente por él, mensaje que fue firmado además por el servidor. Si la respuesta es positiva, verifica la firma del segundo mensaje enviado, obteniendo - *en caso de ser correcta* - la clave de lectura de mensajes enviados por el servidor, id de sesión, el método de compresión y la suite de cifrado seleccionada por este último durante la negociación.

Una vez que el cliente verificó la validez de los mensajes recibidos, le envía al servidor un mensaje de finalización que contiene el identificador de la sesión, la suite de cifrado y el método de compresión, todo cifrado a través del algoritmo irreversible especificado por el servidor en la suite de cifrado y la clave de sesión del cliente.

Al recibir el mensaje, el servidor genera un mensaje nuevo con el id de sesión, el método de compresión y la suite de cifrado. Cifra dicho mensaje a mensaje con un algoritmo de cifrado irreversible *(el algoritmo irreversible presente en la suite de cifrado seleccionada por el servidor en el segundo paso* y la clave de sesión del servidor. Realiza una comparación entre el mensaje cifrado enviado por el cliente y el mensaje cifrado por él. De ser iguales tales mensajes cifrados significa que el cliente recibió toda la información de manera correcta, o sea, fue un éxito la comunicación servidor-cliente.

El cliente necesita estar seguro de que la información recibida no fue modificada en el transcurso de la comunicación. Por esta razón el servidor envía un mensaje de finalización cifrado con el algoritmo irreversible

y su clave de sesión. Dicho mensaje contendría el identificador de la sesión y la suite de cifrado, para ello el servidor envía el mensaje generado por él cifrado con el algoritmo irreversible. Una vez que el cliente recibe el mensaje de finalización, este procede a cifrar con el algoritmo de cifrado irreversible y su clave de sesión un nuevo mensaje conformado por el identificador de la sesión y la suite de cifrado.

En este momento el cliente sabe que está "hablando" con el servidor, del mismo modo, el servidor sabe que está "hablando" con el cliente, además, cada uno conoce la clave que va a usar para cifrar los mensajes a enviar, la clave para descifrar los mensajes recibidos y los mecanismos de cifrado que van a utilizar durante la comunicación.

3.3.3. Cifrar Documento Local

3.3.3.1. Descripción del protocolo

La idea fundamental de este protocolo surge a partir de la necesidad identificada de un usuario de compartir de forma secreta, la información plasmada en un documento con un conjunto de usuarios. En este caso el documento se encuentra almacenado en el disco duro de su ordenador.

De manera general, cada vez que un usuario seleccione en su cliente de Portafirmas Digit@l la opción "Cifrar Documento Local", se ejecutarán las siguientes acciones.

1. Se cifrará el documento a partir de una suite de cifrado seleccionada por el usuario.

2. Se iniciará automáticamente el protocolo de establecimiento de conexión, el cual inicia una sesión o conexión con el servidor, donde se encuentra desplegado el repositorio de contenidos del Portafirmas Digit@l.

3. Se envían de manera secreta los datos resultantes del proceso de cifrado.

4. Se almacenan los datos en el repositorio de contenidos del Portafirmas Digit@l.

3.3.3.2. Requerimientos del protocolo

Para lograr que el documento pueda ser compartido de forma segura al tiempo que se garantiza la confidencialidad de la información que contiene, se establecen los siguientes objetivos:

1. Garantizar la confidencialidad de la información contenida en el documento.
2. Sincronizar el cliente con el servidor.
3. Intercambiar de manera segura/secreta los datos enviados y recibidos tanto por el cliente como por el servidor.
4. Negociar parámetros de sesión en la comunicación cliente-servidor.
5. Poner a disposición de los usuarios el documento cifrado.

Como se puede observar, algunos de los objetivos mencionados anteriormente son resueltos por el protocolo de "Establecimiento de Conexión", de hecho, en cada una de las funcionalidades en las cuales interviene o es necesaria la comunicación entre el cliente y el servidor, será necesario tener en cuenta estos objetivos.

3.3.3.3. Propiedades de seguridad

La principal propiedad de seguridad que se pretende garantizar con este protocolo es:

- Compartición secreta entre varios usuarios de la información contenida en un documento.
- Compartición secreta de las claves de descifrado del documento.

3.3.3.4. Modelado del protocolo

Este protocolo se ejecuta en tres partes fundamentales, en un primer momento, el usuario interactúa con su cliente del Portafirmas Digit@l, luego se envía la información necesaria al servidor en el cual se encuentra el

repositorio de contenido del portafirmas y finalmente se almacena la información en el repositorio; de modo que sea accesible - *solo por los usuarios indicados* - a través de cualquiera de los clientes del portafirmas.

Primera fase

En primer lugar, el usuario selecciona la suite de cifrado y el conjunto de usuarios que tendrán acceso a la información contenida en el documento que se va a cifrar. Una vez seleccionado tales parámetros, el cliente del portafirmas comprime el documento para eliminar la mayor cantidad de redundancia posible, aprovechando además la disminución del tamaño del mismo. Luego se cifra el documento a través de un algoritmo simétrico usando una clave de sesión generada aleatoriamente por un algoritmo generador de claves. Esta clave es cifrada a través de un algoritmo asimétrico y usando las claves públicas de cada uno de los usuarios seleccionados que podrán descifrar dicho documento. Todos los algoritmos utilizados conforman la suite de cifrado selecciona por el usuario.

Segunda fase

Una vez cifrado el documento y la clave de sesión para cada uno de los usuarios seleccionados se inicia el proceso de envío de dichos datos hacia el repositorio de contenidos del Portafirmas Digit@l. Para ello, lo primero es iniciar el Protocolo de Establecimiento de Conexión (EDC). Una vez iniciada una sesión, se envía el documento cifrado y las claves de sesión cifradas firmado a nombre del usuario. Se envía además, firmado a nombre del usuario un mensaje de manera secreta- *cifrado con la clave de sesión de escritura obtenida durante la ejecución del protocolo EDC ejecutado anteriormente y aplicando el algoritmo de cifrado seleccionado en la suite de cifrado durante la ejecución del protocolo EDC*- que contiene la suite de cifrado utilizada para realizar la operación, nombre del propietario del documento, nombre del documento, fecha de la operación.

Tercera fase

En esta fase, el servidor verifica la firma del mensaje envíado por el cliente, de ser válida, almacena en el repositorio de contenidos del Portafirmas Digit@l el documento cifrado junto con las claves de descifrado asociado a cada uno de los usuarios seleccionados. O sea, se almacena en el sistema de ficheros el documento cifrado y las claves de descifrado y se establecen los permisos necesarios para que los usuarios puedan acceder a dicho documento y únicamente a su clave de descifrado correspondiente. Una vez

almacenados los documentos el servidor envía la cliente el mensaje firmado por él. El cliente verifica la validez de la firma, de esta forma comprueba que el servidor recibió la información enviada por él.

Con este protocolo se garantiza que varios usuarios puedan compartir información secreta, cada uno accediendo a la misma con una clave secreta que solamente podrá ser descifrada con su clave privada. Ni siquiera los administradores de red tendrán acceso a la información.

3.3.4. Cifrar Documento en el Servidor

3.3.4.1. Descripción del protocolo

La idea fundamental de este protocolo surge a partir de que un usuario identifica la existencia de un documento con información confidencial que reside en el repositorio de contenidos del Portafirmas Digit@l, expuesto a personas no autorizadas como los administradores del sistema.

De manera general, cada vez que un usuario seleccione en su cliente de Portafirmas Digit@l la opción "Cifrar Documento en el Servidor", se ejecutarán las siguientes acciones.

1. Se iniciará automáticamente el protocolo de establecimiento de conexión, el cual inicia una sesión o conexión con el servidor, donde se encuentra desplegado el repositorio de contenidos del Portafirmas Digit@l.

2. El servidor envía de manera secreta los documentos que se encuentran en el repositorio de contenidos del Portafirmas Digit@l, para que el usuario seleccione cual desea cifrar.

3. El cliente envía al servidor de forma secreta los usuarios que tendrán acceso a la información contenida en el documento y la suite de cifrado seleccionada por el usuario para que realice el cifrado de la información.

4. Se almacenan los datos en el repositorio de contenidos del Portafirmas Digit@l.

5. Se elimina el documento en texto plano.

3.3.4.2. Requerimientos del protocolo

Para restringir el acceso a la información confidencial contenida en determinados documentos y garantizar su confidencialidad se establecen los siguientes objetivos:

1. Garantizar la confidencialidad de la información contenida en el documento.
2. Sincronizar el cliente con el servidor.
3. Intercambiar de manera segura/secreta los datos enviados y recibidos tanto por el cliente como por el servidor.
4. Negociar parámetros de sesión en la comunicación cliente-servidor.
5. Restringir el acceso a documentos con información confidencial. El documento cifrado se encontrará disponible solo para un conjunto determinado de usuarios.

3.3.4.3. Propiedades de seguridad

La principal propiedad de seguridad que se pretende garantizar con este protocolo de seguridad es:

- Restringir el acceso a la información confidencial contenida en un documento.
- Compartición secreta de las claves de descifrado de los documentos.

3.3.4.4. Modelado del protocolo

Este protocolo se ejecuta en tres fases fundamentales, en un primer momento, el usuario interactúa con su cliente del Portafirmas Digit@l y se inicia el Protocolo de Establecimiento de Conexión (EDC). Luego se envía al servidor de manera secreta la suite de cifrado, el documento y el conjunto de usuarios. Finalmente, se procede a cifrar el documento.

Primera fase

El usuario selecciona los usuarios que deberían tener acceso a la información contenida en el documento que se va a cifrar, la suite de cifrado que sé utilizará y se genera un mensaje (denominado contrato) con esta información. Se inicia el Protocolo de Establecimiento de Conexión (EDC) y se envía de manera secreta el contrato al servidor.

Segunda fase

En esta fase, el servidor ha recibido toda la información e inicia el proceso de cifrado del documento. Para ello, el servidor comprime el documento para eliminar la mayor cantidad de redundancias posibles, aprovechando la disminución del tamaño del mismo. Luego, se genera una clave de sesión, que será utilizada por el algoritmo simétrico para cifrar el documento. Esta clave es cifrada por un algoritmo asimétrico con la clave pública de cada uno de los usuarios que podrán descifrar el documento. Los mecanismos utilizados en este proceso son los que conforman la suite de cifrado seleccionada por el usuario.

Tercera fase

Una vez cifrado el documento, se almacena en el repositorio de contenidos del Portafirmas Digit@l el documento cifrado junto con las claves de descifrado asociado a cada uno de los usuarios seleccionados y se elimina el documento en texto plano. Luego el servidor le envía al cliente el contrato firmado a su nombre. El cliente verifica la validez del contrato.

Con este protocolo se garantiza que la información confidencial contenida en documentos no se encuentre expuesta a personas no autorizadas. Solo un conjunto determinado de usuarios seleccionado por el propietario del documento podrán acceder a la información, ya que cada uno posee una clave secreta que solamente podrá ser descifrada con su clave privada.

3.3.5. Descifrar Documento Local

3.3.5.1. Descripción del protocolo

Este protocolo surge a partir de la necesidad que tiene un usuario de obtener para consumo propio la información contendida en un documento cifrado para él o por él que reside en el repositorio de contenidos del Portafirmas Digit@l.

De manera general, cada vez que un usuario seleccione en su cliente de Portafirmas Digit@l la opción "Descifrar Documento Local", se ejecutarán las siguientes acciones.

1. Se iniciará automáticamente el protocolo de establecimiento de conexión, el cual inicia una sesión o conexión con el servidor, donde se encuentra desplegado el repositorio de contenidos del Portafirmas Digit@l.

2. El servidor envía de manera secreta los documentos que se encuentran en el repositorio de contenidos del Portafirmas Digit@l, para que el usuario seleccione cual desea descifrar.

3. El cliente envía al servidor de forma secreta el documento que el usuario desea descifrar.

4. El servidor envía toda la información asociada a la suite de cifrado utilizada para cifrar el documento, incluyendo la clave de sesión con la que fue cifrado el documento.

3.3.5.2. Requerimientos del protocolo

Para obtener la información contenida en un documento para consumo propio del usuario y garantizar su confidencialidad se establecen los siguientes objetivos:

1. Garantizar la confidencialidad de la información contenida en el documento.

2. Sincronizar el cliente con el servidor.

3. Intercambiar de manera segura/secreta los datos enviados y recibidos tanto por el cliente como por el servidor.

4. Negociar parámetros de sesión en la comunicación cliente-servidor.

3.3.5.3. Propiedades de seguridad

La principal propiedad de seguridad que se pretende garantizar con este protocolo es:

- Obtener para consumo propio del usuario la información confidencial contenida en un documento.
- Compartición secreta de las claves de descifrado de los documentos.

3.3.5.4. Modelado del protocolo

Este protocolo se ejecuta en tres fases fundamentales, en un primer momento, el usuario interactúa con su cliente del Portafirmas Digit@l y se inicia el Protocolo de Establecimiento de Conexión (EDC). Luego se envía al cliente de manera secreta la suite de cifrado, el documento cifrado y la clave de sesión cifrada asociada al documento. Finalmente, el cliente descifra el documento.

Primera fase

El usuario selecciona en la barra de herramientas del Portafirmas Digit@l la opción " Descifrar Documento Local" y se inicia el Protocolo de Establecimiento de Conexión (EDC), ya que el usuario necesita obtener los documentos cifrados que residen en el servidor y que él tiene permisos para descifrar. Luego de iniciada la sesión el cliente le envía una petición al servidor de forma secreta, solicitando el listado de documentos que puede descifrar el usuario. El servidor envía de manera secreta el listado de documentos cifrados solicitados por el cliente.

Segunda fase

En esta fase el cliente ha recibido la información solicitada al servidor. El usuario selecciona el documento y el cliente le envía de manera secreta una petición al servidor solicitando el documento y la información asociada al documento, o sea, suite de cifrado y clave de sesión cifrada. El servidor le envía de manera secretra al cliente la información solicitada.

Tercera fase

Una vez que el cliente ha recibido toda la información inicia el proceso de descifrado del documento. Para ello, el cliente descifra la clave de sesión utlizando el mismo algoritmo asimétrico con que fue cifrada y con la clave privada del usuario. Luego, descifra el documento con el mismo algoritmo simétrico con que fue cifrado y con la clave de sesión descifrada. Finalmente, se descomprime el documento con el mismo algoritmo que fue comprimido. Una vez descifrado el documento, se almacena en el disco duro de la computadora del usuario.

Con este protocolo se garantiza que los usuarios con permisos para obtener la información puedan acceder a ella sin hacerla pública. De esta forma, la información continuará cifrada en el repositorio de contenidos.

3.3.6. Descifrar Documento en el Servidor

3.3.6.1. Descripción del protocolo

Este protocolo surge cuando la información de un documento cifrado deja de ser confidencial, se procede a descifrar el documento en el servidor, reemplazando la versión cifrada por el documento original.

De manera general, cada vez que un usuario seleccione en su cliente de Portafirmas Digit@l la opción “Descifrar Documento en el Servidor”, se ejecutarán las siguientes acciones.

1. Se iniciará automáticamente el protocolo de establecimiento de conexión, el cual inicia una sesión o conexión con el servidor, donde se encuentra desplegado el repositorio de contenidos del Portafirmas Digit@l.

2. El servidor envía de manera secreta los documentos que se encuentran en el repositorio de contenidos del Portafirmas Digit@l, para que el usuario seleccione cual desea descifrar.

3. El cliente envía al servidor de forma secreta el documento que el usuario desea descifrar.

4. El servidor envía la clave de sesión con la que fue cifrado el documento.

5. El cliente envía la clave de sesión descifrada.

3.3.6.2. Requerimientos del protocolo

Para hacer pública una información cifrada que se encuentra en el repositorio de contenidos se establecen los siguientes objetivos:

1. Garantizar la confidencialidad de la información contenida en el documento.
2. Garantizar la seguridad de la clave privada del usuario.
3. Sincronizar el cliente con el servidor.
4. Intercambiar de manera segura/secreta los datos enviados y recibidos tanto por el cliente como por el servidor.
5. Negociar parámetros de sesión en la comunicación cliente-servidor.

3.3.6.3. Propiedades de seguridad

La principal propiedad de seguridad que se pretende garantizar con este protocolo es:

- Hacer pública la información cifrada que ha dejado de ser confidencial.
- Compartición secreta de las claves de descifrado de los documentos.

3.3.6.4. Modelado del protocolo

Este protocolo se ejecuta en tres fases fundamentales, en un primer momento, el usuario interactúa con su cliente del Portafirmas Digit@l y se inicia el Protocolo de Establecimiento de Conexión (EDC). Luego se envía al cliente de manera secreta la clave de sesión cifrada asociada al documento y el mecanismo asimétrico utilizado para cifrar dicha clave. Una vez descifrada la clave de sesión, el cliente la envía al servidor para que descifre el documento. Finalmente, se descifra el documento.

Primera fase

El usuario selecciona en la barra de herramientas del Portafirmas Digit@l la opción “Descifrar Documento en el Servidor“ y se inicia el Protocolo de Establecimiento de Conexión (EDC), ya que el usuario necesita obtener los documentos que fueron cifrados por él. Luego de iniciada la sesión, el cliente le solicita de forma secreta al servidor los documentos cifrados. El servidor recibe la solicitud por parte del cliente y procede a enviarle la información de manera secreta.

Segunda fase

En esta fase, el cliente ha recibido la información solicitada al servidor y el usuario selecciona el documento que desea descifrar. El cliente le envía una petición de manera secreta al servidor solicitando la clave de descifrado asociada al documento y el algoritmo asociado para cifrar dicha clave. El servidor le envía al servidor la información solicitada. El cliente recibe la información y procede a descifrar la clave de descifrado del documento. Para ello, se utiliza el mismo algoritmo asimétrico con que fue cifrada y la clave privada del usuario. Al obtener la clave de sesión descifrada el cliente la envía de manera secreta al servidor para que descifre el documento.

Tercera fase

En esta fase el servidor ha recbido la clave y procede a descifrar el documento. Para ello utiliza el mismo algoritmo simétrico con que fue cifrado y la clave de sesión. Finalmente, se descomprime el documento y se reemplaza el documento cifrado por el documento original.

Con este protocolo se garantiza que una información cifrada que ha dejado de ser confidencial pueda ser descifrada en el servidor sin necesidad de transmitir por la red las claves privadas de los usuarios.

3.3.7. Análisis de los protocolos

¿Qué pasa si existe un intruso “escuchando“ toda la comunicación que se establece por el canal?

Si un intruso pasivo logra inmiscuirse en la comunicación, entonces obtendrá toda la información que se envía y recibe por parte de los agentes. Sin embargo, este no será capaz de descifrar ninguno de los datos si no cuenta con el par de claves de sesión generadas durante el establecimiento de la comunicación.

¿Qué pasa si el intruso logra apoderarse de las claves de sesión generadas durante la conexión cliente-servidor?

Si esto ocurre, los protocolos anteriormente descritos garantizan que el intruso no pueda apoderarse de la información cifrada a petición del usuario. En primer lugar, en ninguno de los casos las claves de sesión empleadas para la comunicación cliente-servidor coincidiría con la clave de sesión empleada para cifrar o descifrar el documento. En segundo lugar, una vez que tenga las claves de descifrado de los usuarios, este deberá apoderarse de la clave privada del usuario del cual obtiene su clave de descifrado y solo es de su conocimiento.

¿Qué sucede si un intruso modifica el más mínimo bit en la comunicación?

Los protocolos anteriormente citados garantizan, a través de un mecanismo de verificación de integridad que cualquier cambio ocurrido durante la transmisión de la información sea detectado, de tal manera se tomarían las medidas de seguridad pertinentes para conocer quién es el responsable de tal acto.

Para ver los diagramas asociados a cada uno de los protocolos ver Anexo D de la versión extendida de este documento.

Análisis del capítulo

Los protocolos criptográficos definidos en este capítulo garantizan la confidencialidad de la información y la seguridad de la comunicación entre el cliente y el servidor.

Capítulo 4

Análisis y Diseño

En el actual capítulo se modela el sistema a través de los flujos de trabajo análisis y diseño con el propósito de definir como debe ser implementada la solución. Se define la arquitectura para que soporte todos los requisitos y las restricciones que se le suponen. Incluye además, los diagramas de interacción, los diagramas de clases del diseño, así como las descripciones de cada una de las clases.

4.1. Modelo del análisis

" El modelo del análisis representa los requisitos en múltiples dimensiones, con lo que se incrementa la probabilidad de encontrar errores, de que surjan inconsistencias y de que se descubran omisiones" [21] .

4.1.1. Diagramas de interacción

Un diagrama de interacción es en un conjunto de objeto y sus relaciones, incluyendo los mensajes que pueden ser enviados entre ellos. Tratan la vista dinámica de un sistema; incluyen diagramas de colaboración y diagramas de secuencia [15].

Los diagramas de secuencia destacan el orden temporal de los mensajes, mostrando los objetos que participan en la interacción mediante sus líneas de vida. En el caso de los diagramas de colaboración se resalta la organizacion estructural de los objetos que envían y reciben mensajes.

Para una mejor comprensión del sistema ver Anexo B de la versión extendida de este documento donde se muestran los diagramas de colaboración generados por cada caso de uso y una descripción del flujo de sucesos-análisis que explica cada uno de ellos.

4.2. Arquitectura del sistema

"Una arquitectura es el sistema de decisiones significativas sobre la organización de un sistema de software, la selección de los elementos estructurales y de sus interfaces por los cuales el sistema es compuesto, junto con su comportamiento según lo especificado en las colaboraciones entre estos elementos, la composición de estos elementos estructurales y del comportamiento en subsistemas progresivamente más grandes y el estilo arquitectónico que dirigen esta organización, los elementos y sus interfaces, sus colaboraciones y su composición" [15].

El Portafirmas Digit@l tiene una arquitectura n-capas. Las cuales se explicarán a continuación.

4.2.1. Capa de Datos/Almacenamiento físico

La Capa de Datos/Almacenamiento físico es denominada comúnmente repositorio de contenidos. Hace referencia al lugar donde se almacena toda la información. Consiste en una jerarquía de nodos de diferentes tipos, cada nodo se encuentra asociado a un nodo padre a través de la relación padre-hijo, con la excepción del nodo raíz que no tiene padre. Un nodo puede relacionarse con otros nodos a partir de la definición de asociaciones.

Básicamente, el repositorio de contenidos se compone de un conjunto de almacenes (stores) en los cuales residen los nodos. Cada almacén concentra la información asociada a una lógica de negocio o de aplicación en particular. Los almacenes a su vez pueden residir en una base de datos (así es como ocurre normalmente) o físicamente en el disco duro. El Portafirmas Digit@l hace uso de dos almacenes fundamentales:*Working Store* (espacio de trabajo) y *Content Store* (almacén de contenidos).

El espacio de trabajo *Working Store*, mejor conocido como *Spaces Store* (almacén de espacios) concentra toda la información relacionada con los procesos que se ejecutan desde el Portafirmas Digit@l u otras aplicaciones o clientes. Para ello se hace uso de otras estructuras jerárquicas de segundo nivel, más conocidas como Raíz o Root, tal es el caso de *NotificationRoot* (para la gestión de notificaciones), *SharedRoot* (para la gestión de recursos compartidos) y *CategoryRoot* (para la gestión de categorías), entre otros.

El almacén de contenidos, *Content Store* o Sistema de ficheros, es actualmente el único que se aloja fuera del contexto del Sistema de Bases de datos. En este se almacena toda la información que se dispone en formato binario. Se divide o estructura en diferentes carpetas que funcionan de la misma manera que las raices en el almacén *Spaces Store*. Sus estructuras fundamentales son *conten-store* (para la gestión de los documentos en formato binario), *lucene-indexes* (para la gestión de los índices de lucene), *key-store* (para la gestión de los certificados digitales de cada uno de los usuarios).

4.2.2. Capa de Acceso al Repositorio

La Capa de Acceso al Repositorio contiene los módulos, librerías y clases que permiten obtener y modificar la información que se almacena en el repositorio de contenidos. Sus componentes se estructuran en paquetes o subsistemas de servicios, cada uno de los cuales proporcionan un conjunto coherente de funcionalidades reutilizables, de modo que las aplicaciones adquieren una combinación adecuada de funciones para llevar a cabo cierta lógica de negocio.

Los dos subsistemas fundamentales que incorpora el Portafirmas Digit@l en esta capa son *PKI Service* (Servicios de infraestructura de clave pública) y *Signature Service* (Servicios de firma digital). El primero es el encargado de interactuar con una infraestructura de Clave Pública (PKI) para el manejo de los certificados digitales de los usuarios (obtención, validación, almacenamiento, entre otros). Por otra parte, *Signature Services* es el subsistema encargado de brindar las funcionalidades necesarias para llevar a cabo el procedimiento de firma digital de documentos y sobre todo la validación de la firma del lado del servidor.

4.2.3. Capa de Aplicación-Servidor

La Capa de Aplicación-Servidor tiene como principal responsabilidad proveer un conjunto de servicios que pueden ser usados por sistemas o clientes externos al contexto del servidor para la construcción e implementación de nuevas aplicaciones. Se exponen de esta manera un conjunto de interfaces públicas que permiten la comunicación de terceras aplicaciones con el repositorio de contenidos. La diferencia

fundamental entre esta capa y la capa de Acceso al Repositorio es que todos sus servicios son públicos y pueden ser consumidos por clientes externos.

El Subsistema de Servicios o interfaces públicas de esta capa más importante, en el contexto del Portafirmas Digit@l, es *WebService Security FrameWork* cuyo objetivo es poner a disposición de sistemas externos las principales funcionalidades que brinda el subsistema *Signature Service* de la capa de Acceso al Repositorio a través de una comunicación segura a nivel de aplicación.

4.2.4. Capa de Aplicación-Cliente

La Capa de Aplicación-Cliente tiene como principal objetivo brindar un conjunto de funcionalidades y servicios de aplicación necesarios para la construcción de aplicaciones que necesiten comunicarse con el repositorio de contenidos del Portafimas Digit@l. Los subsistemas fundamentales en esta capa son el Subsistema de Comunicación con la capa de Aplicación- Servidor, el Subsistema de firma digital (*Signature Service*) y el Subsistema de Gestión de Certificados (*PKI Service*).

El Susbsistema de Comunicación con la capa de Aplicación-Servidor como su nombre lo indica, provee las interfaces y funciones necesarias para iniciar una comunicación con el repositorio de contenidos de manera segura a nivel de aplicación. El Subsistema de firma digital brinda las funciones necesarias para llevar a cabo la aplicación de la firma digital desde una aplicación cliente y el Subsistema de Gestión de Certificados permite gestionar los certificados digitales de cada uno de los clientes registrados en el sistema.

4.2.5. ¿Cómo se inserta el módulo de cifrado de documentos en la arquitectura del Portafirmas Digit@l?

4.2.5.1. Capa de Datos/Almacenamiento físico

En el almacén *Working Store* se propone adicionar una nueva raíz (root) denominada *CipherRoot*. En esta raíz se almacenará la información asociada a los documentos cifrados que se incorporen al repositorio de contenidos (nombre del documento, conjunto de claves de sesión cifradas, entre otros datos).

En el almacén de contenidos, *Content Store*, se almacenarán las claves de sesión como documentos binarios, en un nuevo espacio denominado *Cipher-store*.

4.2.5.2. Capa de Acceso al Repositorio

En la Capa de Acceso al repositorio se propone adicionar un nuevo subsistema de servicios denominado *Cipher Services* que contendrá las funcionalidas para realizar las operaciones de cifrado de documentos desde el propio servidor.

4.2.5.3. Capa de Aplicación-Servidor

En la Capa de Aplicación-Servidor se propone incluir los servicios necesarios para que las aplicaciones externas puedan solicitar la ejecución de las nuevas funcionalidades que se incorporan en la capa de Acceso al Repositorio a través del Subsistema *Cipher Services*.

4.2.5.4. Capa de Aplicación-Cliente

En la Capa de Aplicación-Cliente se propone incorporar un nuevo subsistema denominado *Client-Cipher-Services*, que incluirá las funcionalidades necesarias para ejecutar de manera segura (a nivel de aplicación) los servicios que exporta la Capa de Aplicación-Servidor, relacionados con el nuevo subsistema incorporado.

4.2.5.5. Capa de Presentación (Portafirmas Digit@l)

La Capa de Presentación (Portafirmas Digit@l) incluye el Subsistema *Cipher-Application* que contiene las clases que controlan el proceso de cifrado de los documentos, generación de claves de sesión, entre otros. Además, se propone incorporar las clases de Interfaz de usuario necesarias para la interacción del usuario con la aplicación.

Para ver la imagen de la arquitectura ver anexo G de la versión extendida de este documento.

4.3. Modelo de diseño

"El modelo de diseño es un modelo de objetos que describe la realización física de los casos de uso centrándose en cómo los requisitos funcionales y no funcionales, junto con otras restricciones relacionadas con el entorno de implementación, tienen impacto en el sistema a considerar "[15].

Para ver los diagramas de secuencia ver Anexo B de la versión extendida de este documento.

4.3.1. Patrones de diseño

Los patrones de diseño ofecen una solución a problemas específicos y comunes del diseño orientado a objetos en el proceso de desarrollo de software. Un ejemplo de patrones son los GRASP (General Responsibility Asignment Software Patterns) que describen los principios de asignar responsabilidades a objetos para lograr un diseño eficaz del software [22].

- **Controlador**: asigna la responsabilidad de las operaciones del sistema a 1os objetos situados en la capa del dominio y no en 1os soportes de la capa de presentación [22]. La utilización de este patrón se evidencia cuando la clase interfaz UI_CifrarDocumentoLocal, que forma parte de la capa de Presentación, envía los datos para la clase controladora Coontrolador, que se encarga de ejecutar los flujos de operaciones. Con la aplicación de este patrón se logra un mejor control y potencialidad de los componentes reutilizabes, ya que los procesos relacionados con los flujos de operaciones no son manejados por la capa interfaz, sino por la capa de aplicación,

- **Bajo Acoplamiento:** su función es asignar responsabilidad para mantener bajo acoplamiento. El acoplamiento consiste en la fuerza con que una una clase está conectada a otras clases. Una clase con bajo acoplamiento no depende de muchas otras [22]. Un ejemplo de la aplicación de este patrón es en la clase CipherServices, ya que si se le realiza algún cambio no afecta a las otras clases y se obtendrá el mismo resultado. Esto sucede con todas las clases.

- **Alta Cohesión:** asigna responsabilidad de manera tal que la cohesión siga siendo alta. Una alta cohesión caracteriza a las clases con responsabilidades estrechamente relacionadas que no realicen un trabajo

enorme [22]. Este patrón está relacionado con el patrón bajo acoplamiento por lo que el ejemplo de su utilización es el mismo. Con este patrón se logra mayor capacidad de reutilización, ya que cada clase tiene su propósito específico.

4.3.2. Clases del diseño

Una clase del diseño es una abstracción de una clase o construcción similar en la implementación del sistema. El lenguaje utilizado por estas clases debe ser igual al lenguaje de programación que se utilizará en la implementación del sistema, especifican atributos y operaciones.

La siguiente figura muestra el diagrama de clases de diseño de la solución que se propone. En él se muestran las principales clases e interfaces que modela el sistema.

Para ver el diagrama de clases del diseño ir al anexo E de la versión extendida de este documento.

4.3.2.1. Descripción de las clases del diseño

Nombre: UI_Principal	
Tipo de clase: Interfaz	
Para cada responsabilidad	
mostarUI_CifrarDocumentoLocal()	Muestra el cuadro de diálogo UI_CifrarDocumentoLocal.
mostraUI_CifrarDocumentoServidor()	Muestra el cuadro de diálogo UI_CifrarDocumentoServidor.
mostraUI_DescifrarDocumentoLocal()	Muestra el cuadro de diálogo UI_DescifrarDocumentoLocal.
mostraUI_DescifrarDocumentoServidor()	Muestra el cuadro de diálogo UI_DescifrarDocumentoServidor.
Continúa en la próxima página	

Tabla 4.1: Clase: UI_Principal

Para ver el resto de las descripciones de las clases del diseño ir al anexo F de la versión extendida de este documento.

Análisis del capítulo

Con el desarrollo de este capítulo, los requisitos tanto funcionales como no funcionales se han ido transformando a una especificación que describe como implementar la solución de cifrado desde el Prtafirmas Digit@l. Se ha refinado y definido la arquitectura, quedando sentada las bases para la futura implementación de la solución.

Conclusiones

- El cifrado de documentos es un aspecto no incluido en la mayoría de los portafirmas digitales, por lo que constituye una novedad incluirlo como parte de las funcionalidades de la herramienta Portafirmas Digit@l.
- A través de las técnicas de captura de requisitos aplicadas se identificaron las principales necesidades y funcionalidades que deberían incorporarse a la solución en general.
- Una vez especificados los requisitos como casos de uso del sistema se definieron los protocolos criptográficos que se deben llevar a cabo para garantizar la seguridad del sistema de cifra.
- El diseño del módulo de cifrado constituirá la base fundamental para la implementación del mismo, contribuyendo así a garantizar la confidencialidad de la información que se almacena en el repositorio de contenidos del portafirmas.

Recomendaciones

- Continuar el estudio relacionado con los protocolos criptográficos, sistemas de distribución de claves.
- Aplicar métodos formales de análisis de los protocolos criptográficos.
- Implementar la solución teniendo en cuenta la propuesta presentada.

Referencias bibliográficas

[1] GUTIÉRREZ J and IBÁÑEZ J and ELORRIAGA J. Cifrado de la información. [Consultado: marzo 2012].

[2] Diccionario de la lengua española - vigésima segunda edición. URL `http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=criptograf%C3%ADa`. [Consultado: enero 2012].

[3] Xifré Solana, Patricia. *Antecedentes y perspectivas de estudio en historia de la Criptografía*. PhD thesis, Universidad Carlos III de Madrid, 2008.

[4] Ramió Aguirre, Jorge . *Libro Electrónico de Seguridad Informática y Criptografía*. URL `http://www.criptored.upm.es/guiateoria/gt_m001a.htm`. [Consultado: Enero 2012].

[5] Gómez Aguilar, Diego Alonso and García Navarro, Juan Francisco. *Mecanismo de seguridad de la información en aplicaciones web*. PhD thesis, Universidad de Salamanca, 2006.

[6] Lucena López, Manuel J. *Criptografía y seguridad en computadores*. PhD thesis, Escuela Politécnica Superior e Universidad de Jaén, 2006.

[7] Martínez Silva, Nury Mercedes. *Estudio monográfico sobre técnicas de criptografía*. Ingeniería en Ciencias de la computación, Universidad Don Bosco, 2004.

[8] Gestión de claves. http://www.iec.csic.es/criptonomicon/seguridad/claves.html. URL `http://www.iec.csic.es/criptonomicon/seguridad/claves.html`. [Consultado: marzo 2012].

[9] Servicios de seguridad. http://www.iec.csic.es/criptonomicon/seguridad/servicio.html. URL `http://www.iec.csic.es/criptonomicon/seguridad/servicio.html`.

[10] Rankl W and Effing W. *Smart Card Hanbook*. ISBN 0471988758.

[11] Vicerrectorado de tecnologías de la información y la comunicación. *Evaluación y revisión*. PhD thesis, Universidad Pablo de Olavide, De Sevilla, 2009.

[12] Port@firmas | portal de administración electrónica. URL `https://ws024.juntadeandalucia.es/ae/adminelec/areatecnica/portfirmas`. [Consultado: marzo 2012].

[13] Area de tecnologías de la información y las comunicaciones aplicadas de la universidad de murcia (ATICA) - portafirmas de documentos electrónicos. URL `http://www.um.es/atica/portafirmas`. [Consultado: marzo 2012].

[14] Agenda de firmas electrónicas - viafirma inbox | viafirma. URL `http://www.viafirma.com/es/node/2`. [Consultado: marzo 2012].

[15] Jacobson Ivar, Booch Grady and Rumbaugh James. *El proceso unificado de desarrollo de software*, volume 1. Félix Varela, 2000. ISBN 84-7829-036-2.

[16] El documento electrónico en el derecho civil chileno: Análisis de la ley 19.799. URL `http://www.scielo.cl/scielo.php?pid=s0718-00122004000200005&script=sci_arttext`. [Consultado: febrero- 2012].

[17] UNE-ISO. *especificación de Moreq*. [Consultado: Enero 2012].

[18] Sommerville, Ian. *Ingeniería del software*. séptima edition. ISBN 84-7829-074-5. [Consultado: febrero 2012].

[19] Fernando López Hernández. Seguridad, criptografía y comercio electrónico con java.

[20] Tobarra Abad, María de los Llanos. *Formals methods for the analysis of security protocols*. Doctoral, University of Castilla-La Mancha, 2009.

[21] Pressman, Roger. *Ingeniería del Sosftware: Un Enfoque Práctico*. ISBN 0471988758.

[22] Larman Craig. *UML y PATRONES : Introducción al análisis y diseño orientado a objetos*. Felix Varela, La Habana, 2004.

Bibliografía

- Martínez Silva, Nury Mercedes, "*Estudio monográfico sobre técnicas de criptografía*", Ingeniería en Ciencias de la computación, Universidad Don Bosco, 2004.
- Alor Osorio, Juan Manuel. "*Evaluación de la herramienta EJBCA para un Prestador de Servicios de Certificación*", Universidad Politécnica de Cataluña.
- Gayoso Martínez,Víctor. "*Implementación en tarjetas inteligentes Java Card de protocolos de cifrado y descifrado basados en curvas elípticas*". Universidad Politécnica de Madrid,2010.
- García Eugenio, López Miguel Ángel and Ortega Jesús J. "*Una introducción a la criptografía*".
- Lucena López, Manuel José . "*Criptografía y Seguridad en Computadores*". Universidad de Jaén, 2006.
- Death Master, "*Introducción a la Esteganografía*".
- Jacobson Ivar, Booch Grady and Rumbaugh James. "*El proceso unificado de desarrollo de software*", isbn= 84-7829-036-2, volume = 1, editorial: Félix Varela.
- López Hernández, Fernando, "*Seguridad, criptografía y comercio electrónico con Java*".
- Tábarae, José Luis . "*Breve Historia de la Criptografía Clásica*".
- Pressman, Roger "*Ingeniería del Sosftware: Un Enfoque Práctico*", isbn = 9701054733,
- Ramió Aguirre, Jorge. "*Libro Electrónico de Seguridad Informática y Criptografía*",

- Gómez Aguilar, Diego Alonso, García Navarro, Juan Francisco. "*Mecanismo de seguridad de la información en aplicaciones web*". Universidad de Salamanca. 2006
- UNE-ISO. "*Especificación de Moreq*", [Consultado: Enero 2012].
- Xifré Solana Patricia . "*Antecedentes y perspectivas de estudio en historia de la Criptografía*". Universidad Carlos III de Madrid, 2008
- Rumbaugh James, Jacobson Ivar, Booch Grady . "*El lenguaje Unificado de Modelado*".
- Servicios de seguridad, [Consultado marzo 2012]. Disponible en la direccion web: "http://www.iec.csic.es/criptonomicon/seguridad/servicio.html".
- Sommerville Ian . "*Ingeniería del software*", isbn = 84-7829-074-5.
- Rankl W, Effing W. "*Smart Card Hanbook*", isbn = 0471988758.
- García Rojas Walter Augusto,"*Implementación de Firma Digital en una plataforma de comercio electrónico*". Universidad Católica del Perú, 2008.
- Documento electrónico, [Consultado marzo 2012]. Disponible en la direccion web: "http://www.scielo.cl/scielo.php?pid=s0718-00122004000200005&script=sci_arttext".
- Miatello Leonardo, "*Firma y documento digital. Su desarrollo, teórico, técnico y legislativo.*". Universidad de BELGRANO, 2003.
- Vicerrectorado de tecnologías de la información y la comunicación evaluación. "*Evaluación y revisión*". Universidad Pablo de Olavide, De Sevilla, 2009
- Gestión de claves, [Consultado marzo 2012]. Disponible en la direccion web: "http://www.iec.csic.es/criptonomicon/seguridad/claves.html".

- Galende Díaz Juan Carlos. ”*Sistemas criptográficos empleados en Hispanoamérica*“.ISSN: 1132-8312
- Port@firmas | Portal de Administración Electrónica,[Consultado marzo 2012]. Disponible en la direccion web:

  "https:
  //ws024.juntadeandalucia.es/ae/adminelec/areatecnica/portfirmas".
- Area de Tecnologías de la Información y las Comunicaciones Aplicadas de la Universidad de Murcia,[Consultado marzo 2012]. Disponible en la direccion web:

  "http://www.um.es/atica/portafirmas".
- Agenda de firmas electrónicas - Viafirma Inbox,[Consultado marzo 2012]. Disponible en la direccion web: "http://www.viafirma.com/es/node/2".
- Visual Paradigm, [Consultado febrero 2012]. Disponible en la direccion web: "http://www.freedownloadmanager.org/es/downloads/Paradigma_Visual_para_UML_(Iglesia_Anglicana)_para_Windows_14718_p/".
- Tobarra Abad, María de los Llanos. *Formals methods for the analysis of security protocols*. University of Castilla-La Mancha, 2009.
- Tutorial Visual Paradigm, [Consultado febrero 2012]. Disponible en la direccion web: "http://www.scribd.com/doc/36636137/Tutorial-Visual-Paradigm".