Universidad de las Ciencias Informáticas

Facultad 2

Análisis y Diseño de una aplicación para la protección de contenido en dispositivos móviles.

Trabajo de Diploma para optar por el título de
Ingeniero Informático

Autor: Norbelis Leyva Montero

Tutores: Ing. Daimara Martínez Borrell.
Lic. Noel García Guimeras.

Ciudad de la Habana, Junio de 2008

DECLARACIÓN DE AUTORÍA

Declaramos ser autores de la presente tesis y reconocemos a la Universidad de las Ciencias Informáticas los derechos patrimoniales de la misma, con carácter exclusivo.

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

<nombre autor>	**<nombre tutor>**	**<nombre tutor>**
_____	_____	_____
Firma del Autor	Firma del Tutor	Firma del Tutor

DATOS DE CONTACTO

Daimara Martínez Borrell.
Ingeniera en Ciencias Informáticas, 2007, Universidad de las Ciencias Informáticas.

Noel García Guimeras.
Licenciado en Ciencia de la Computación, 2003, Universidad de La Habana.
Su trabajo de diploma estuvo dedicado a la segmentación de la red vascular en imágenes digitales de retina humana.
Participó en la implementación del proyecto Observatorio de Recursos Humanos de la Escuela Latinoamericana de Medicina (ELAM).
Actualmente trabaja en el desarrollo de software para dispositivos móviles. Ha participado en la implementación del API de Java SAMS-M (JSR-212), en la plataforma de gestión de contenidos para móviles Mobistore, y en la plataforma para la gestión de mensajes Blueeye.
Ha participado en eventos nacionales como COMPUMAT 2005, y eventos internacionales como el XII Congreso Internacional de Computación
(2003) y el 11no Congreso Iberoamericano de Reconocimiento de Patrones (2006). Sus trabajos han sido publicados como parte de estos eventos.
Actualmente cursa la maestría en Informática Aplicada, en la Universidad de Ciencias Informáticas (UCI).

Agradecimientos

Quiero agradecer la culminación de este trabajo a mi mamita y mi papito lindos, quienes me inculcaron el amor por el estudio, porque de ellos aprendí más que de cualquiera de mis queridos y magníficos profesores en toda mi carrera estudiantil, con su ejemplo de trabajo duro, humilde y honrado, los amo; a mi familia, gracias por su protección y guía, por todo el apoyo que siempre me brindan.

A mis tutores, Noel y Daimara por su excepcional capacidad y caudal de conocimientos, pero particularmente por el cariño, la transparencia y amor con que acogieron. A Darién, Arián, Pla, Pedro, gracias a todos por soportarme!!!

A mis amigas, por ser mi familia durante estos cinco años, las hermanas que nunca tuve; a todos mis maestros y profesores, amigos y compañeros de grupo que me han ayudado a ser mejor profesional, pero sobre todo, mejor ser humano.

A Roly, gracias por tu cariño y sobre todo por enseñarme a confiar en mi.

A ustedes, mi gratitud infinita.

Dedicatoria

A quienes siempre deberé un poco más de cuanto pueda lograr
y siempre entregaré más de cuanto posea:
Mis padres.

Resumen

El presente trabajo es el resultado de la investigación detallada del funcionamiento de la tecnología de Administración de Derechos Digitales (DRM). Los sistemas para administración de derechos digitales representan una vía que facilita el acceso controlado a contenidos de tipo texto, audio o vídeo, y por tanto, posibilitan la aparición de nuevos modelos de negocio sobre el acceso y uso de los mismos.

Este documento recoge los resultados obtenidos en el desarrollo del trabajo. Se presentan las principales características de la tecnología DRM. Además, se realiza el análisis y el diseño del Módulo de Administración de Derechos Digitales de la Plataforma de Gestión de Contenido, entrada fundamental de la futura implementación; donde dicha solución es el resultado de la aplicación de la metodología propuesta por Rational Unified Process.
Se establecen las conclusiones obtenidas del desarrollo del trabajo y a partir de esto, se realizan una serie de recomendaciones, que deben ser tomadas en cuenta para posteriores versiones del producto.

Se espera que la solución contribuya a mejorar las prestaciones de servicios de la empresa Cubacel, garantizando a diferentes proveedores la posibilidad de distribuir sus contenidos de forma segura.

Palabra clave

Administración de Derechos Digitales.

Tabla de Contenidos

Introducción

Con el avance de las Tecnologías de la Información y las Comunicaciones (TIC), existe una tendencia a amenazar la integridad de los derechos de propiedad intelectual, pero al mismo tiempo surgen y se implementan nuevas ideas, enfocadas en su protección, garantizando a los medios digitales la distribución de los contenidos de un modo más seguro.

Con la aparición de los dispositivos de entretenimiento portátiles tales como los teléfonos celulares, iPod, palms entre otros, el incremento de los copiadores de CD y DVD y el constante intercambio de archivos entre usuarios a través de Internet, la industria del entretenimiento ha librado una dura batalla contra la piratería y las descargas ilegales de contenido. El esfuerzo más reciente se denomina Administración de Derechos Digitales (del inglés Digital Rights Management [DRM]).

La cual es un conjunto de tecnologías que proporcionan los medios para controlar la distribución y el consumo del contenido digital. (1)

El contenido en formato digital puede ser copiado con gran fidelidad y a diferencia de los medios físicos (como las copias xerográficas y otras) las copias de otras copias son casi tan nítidas y fieles como el original, todas estas tecnologías constituyen a la vez, una herramienta muy valiosa y un potencial peligro para el negocio de la venta de contenidos digitales. De una parte, posibilitan llegar a un mercado inmenso, con unos costes muy bajos, lo que repercute en cuantiosos beneficios para las compañías inmersas en este negocio. Pero por otra parte, facilitan el intercambio, copia, distribución e incluso comercio ilegal, de estos contenidos digitales, suponiendo una grave amenaza para los ingresos de la industria. Esta situación condujo a que las grandes compañías comenzaran a buscar soluciones al problema, mediante tecnologías que les permitieran usar toda la potencia de Internet, pero que a su vez protegieran los derechos de los propietarios legales de los contenidos digitales. De esta forma aparecen las primeras propuestas de tecnologías DRM.

De forma más explicita, DRM puede entenderse como la suma de tecnologías, que protegen la propiedad intelectual de los propietarios de los contenidos digitales, asegurando el uso de estos contenidos de acuerdo a los derechos adquiridos por el consumidor. Cualquier contenido protegido por DRM, sólo puede ser usado según las reglas de consumo adquiridas

por el cliente, que no son más que los derechos de uso, habitualmente contenidos en una licencia.

La descarga de contenido a un teléfono celular, o la recepción de contenidos por los servicios de mensajería, se han convertido en unos de los más populares dentro de los servicios para datos móviles, denominados Servicios de Valor Agregado (del inglés Valor Aggregated Services [VAS]).

Los VAS se gestionan mediante las Plataformas de Entrega de Contenido (*del inglés Content Delivery Platform* [CDP]) las cuales dependiendo del modo de entrega se clasifican en 3 grupos: SMS, IVRs y portales WAP.

Como resultado, dichos servicios deben garantizarle al usuario final la entrega de contenido en un modo fiable independientemente del canal o dispositivo que se utiliza; donde su lógica de negocio debe apoyar los diversos derechos de autor y licencias, hecho que se garantiza mediante el uso de la tecnología DRM.

Como parte de la introducción de nuevos servicios al desarrollo de la informática y las telecomunicaciones en Cuba, a partir de la instalación y puesta en marcha de la plataforma GPRS, la Dirección Central de Servicios Móviles [DCSM] se propone implementar el acceso al portal WAP de la empresa Cubacel a los clientes del servicio de telefonía celular. Actualmente la DCSM cuenta con un portal WAP pero se le hace necesario contar con una aplicación y/o plataforma capaz de manejar los contenidos, en dependencia de los servicios que determine brindar a los clientes. Partiendo de las diferentes vías a través de las cuales se tiene concebido realizar la venta de contenidos, se hace imprescindible dar a conocer los requerimientos para que los mismos sean desarrollados por especialistas de la UCI, para ello se cuenta con la plataforma de Gestión de contenido para dispositivos móviles desarrollada en el Polo de Telecomunicaciones de la facultad 2 de la Universidad de las Ciencias Informáticas, la cual cuenta con el Módulo de administración de derechos digitales encargado de la protección de contenido distribuidos por diferentes proveedores que carecen de un modo de protección de derecho de autor para los mismos.

Como **Objeto de estudio** de este trabajo se analizará la tecnología de Administración de Derechos Digitales, de donde se deriva que el **Campo de Acción** se ajusta a la aplicación de la tecnología DRM en dispositivos móviles.

Teniendo en cuenta lo anteriormente expuesto el **problema científico** queda formulado de la siguiente forma: ¿Cómo diseñar un sistema de administración de derechos digitales para la Plataforma de Gestión de contenido para dispositivos móviles mediante la aplicación de la tecnología DRM?

Se ha propuesto como **objetivo general**: Realizar el análisis y diseño del Módulo de Administración de Derechos Digitales mediante la aplicación de la tecnología DRM que permita gestionar la protección de contenido para dispositivos móviles**.**

Como **objetivos específicos** se plantea:

- Realizar el estudio del estado del arte de la tecnología DRM.
- Definir la metodología para el desarrollo de la solución.
- Definir las herramientas y lenguajes a utilizar.

Para dar cumplimiento a los objetivos trazados se desarrollaron las siguientes **tareas**:

- Realizar una investigación detallada de la tecnología DRM y su aplicación en teléfonos celulares.
- Documentar tecnologías y herramientas a utilizar para el desarrollo de la solución.

Posibles resultados: El diseño del Módulo de Administración de Derechos Digitales para la plataforma de Gestión de contenido para dispositivos móviles.

El documento se estructura en 5 capítulos, representándose todo lo relacionado con el trabajo investigativo realizado, así como la solución al problema planteado.

El primer capítulo “Fundamentación Teórica” está dedicado al estudio de la tecnología DRM, su estructura, la tecnología usada para su programación, entre otros. Los aspectos tratados en este capítulo ayudarán a comprender el proceso de protección de contenido para dispositivos móviles.

El segundo capítulo “Características del Sistema” muestra la modelación del negocio a través modelo de dominio. También se enumeran los requisitos funcionales y no funcionales, se

especifican las características del software, a través de la definición del actor y la descripción de los Casos de Uso.

El tercer capítulo “Análisis y Diseño” donde se muestran los diagramas de clases del análisis y del diseño con sus diagramas de interacción correspondientes.

En el cuarto capítulo “Estudio de la factibilidad” se hace un análisis de las variables de tiempo, costo y esfuerzo y se enuncian además los beneficios tangibles e intangibles que aporta el sistema.

Capítulo1

Fundamentación Teórica

1.1. Introducción.

En el presente capítulo se abordarán temas relacionados con el sistema propuesto. Se hace alusión a los conceptos fundamentales asociados al dominio del problema y los procesos que se relacionan con el objeto de estudio y el campo de acción del trabajo. Se aborda además, un estudio de las tendencias, tecnologías y metodologías más usadas en la actualidad y se concluye con la sección de las herramientas a utilizar durante el proceso de diseño de la aplicación.

1.2. Telefonía Celular.

El teléfono celular es, en nuestros días, el medio de comunicación principal a nivel mundial, y el que más espacios y entornos abarca por sus características trascendentales de tamaño, las mismas, le han dado el seudónimo de móvil, el cual es altamente descriptivo.

Surge en primera instancia como un medio de resolver la necesidad básica de la comunicación a distancia de una manera práctica que permitiera la movilidad del instrumento. Sin embargo, en la actualidad el celular se ha transformado en un objeto personal, y más aún, un accesorio de moda. Además de la comunicación telefónica el celular ofrece a su propietario una amplia gama de propuestas y servicios tendientes a satisfacer diferentes tipos de necesidades. En este contexto, la creciente demanda dentro de la población y la gran cantidad de servicios móviles que proponen las empresas que proveen los servicios conducen a crear una nueva identidad personal de los usuarios. El teléfono además de un instrumento de comunicación, es un objeto de entretenimiento; todo ello en el marco de los últimos adelantos tecnológicos. Algunos de los usos alternativos del teléfono móvil son agenda, despertador, calculadora, cronómetro, juegos, teléfono, mensajes de texto, cámara de fotos y video, servicio de emergencias, televisión en tiempo real, Internet, pantallas color, entre otros. (2)

Con todo esto es fácil imaginar el por qué la finalidad del teléfono celular se ha trasladado de un medio de comunicación a un centro de entretenimiento, y cuya adquisición no siempre implica la necesidad intrínseca de comunicarse, sino de beneficiarse con las ventajas tecnológicas que posee.

La vinculación con la Internet es una ventaja clave de los móviles que el mercado actual ofrece, ya que el desarrollo de ambas tecnologías se da de manera binaria, siendo casi imposible imaginar la una sin la otra.

Normalmente, los contenidos se pueden encontrar desprotegidos en Internet, en las PCs, en los terminales móviles o en otro tipo de dispositivos, y el usuario puede distribuirlo una vez que este se encuentra en su dispositivo sin demasiada complejidad. Esto implica que el proveedor del contenido y el operador pierden el control sobre su uso.

La tecnología DRM, tiene como objetivo dar una respuesta a la problemática asociada a la gestión de los derechos digitales sobre los contenidos. Mediante la aplicación de esta tecnología en el entorno móvil se establecen los procedimientos para permitir la distribución controlada de contenidos y evitar el uso fraudulento.

1.3. Administración de Derechos Digitales.

Administración de Derechos Digitales se puede definir como la suma de tecnologías, herramientas y procesos que protegen la propiedad intelectual durante las operaciones comerciales realizadas con contenidos digitales, considerándose el elemento fundamental del mercado emergente de los contenidos en el entorno móvil.

La aparición de estos sistemas en la esfera del derecho internacional data de diciembre de 1996, teniendo su acomodo legal en el tratado aprobado por la comunidad internacional en el seno de la OMPI (Organización Mundial de la Propiedad Intelectual). Con la incorporación del tratado OMPI en la directiva comunitaria, conocida como de derechos de autor en Internet, lo que se ha hecho es establecer una protección legal específica para estos nuevos medios.

Desde una perspectiva funcional, Administración de Derechos Digitales tiene un significado distinto para gente distinta. Aunque para algunos sólo es el proceso técnico que permite proporcionar contenidos seguros en forma digital, para otros es todo el proceso técnico que permite el intercambio de derechos y contenidos sobre redes, como por ejemplo Internet. A menudo DRM se divide en dos áreas funcionales:

- La identificación y descripción de la propiedad intelectual, los derechos de las obras y de partes implicadas en aspectos administrativos (gestión de derechos digitales)
- La observancia (técnica) de restricciones para su utilización (gestión digital de derechos).

Por lo tanto, la DRM puede hacer referencia a tecnologías y/o procesos aplicables al contenido digital para describirlo e identificarlo y/o para la definición, aplicación y observancia de reglas de utilización de forma segura. (3)

Un sistema completo de gestión de derechos de propiedad intelectual incluye el procesamiento de toda la información sobre los derechos para la administración electrónica de los mismos, incluyendo, a veces, información contractual y personal que permita la gestión extremo a extremo de todos los derechos a lo largo de la cadena de valor. Por su propia naturaleza, DRM puede requerir el acceso a información comercialmente sensible (en contraposición a información de copia y señalización de utilización). La utilización de dicho sistema permite un control muy granular del contenido, permitiendo que los titulares de los derechos apliquen modelos de uso sofisticados.

Este proceso implica inevitablemente una amplia utilización de tecnologías DRM. Dichas tecnologías pueden estar integradas en numerosos componentes, desde los que residen en un único dispositivo, como por ejemplo un Asistente Digital Personal (PDA, Personal Digital Assistant), a los que pueden encontrarse en servidores comerciales en Internet explotados por grandes compañías y organizaciones; independientemente del medio donde se use, su funcionamiento está enmarcado en un solo objetivo, la gestión de derechos de propiedad intelectual. (3)

1.4. Funcionamiento de DRM.

El sistema DRM ideal es flexible, totalmente transparente para el usuario, y complejo para que los maneje un ordenador. El software de primera generación DRM se limitaba simplemente a controlar las copias. La segunda generación DRM todavía está evolucionando y tiene como meta controlar el uso, copiado, impresión, alteración y todo lo que es posible hacer con el contenido digital.

Un escenario típico DRM opera a tres niveles: Establecer un copyright (derecho de copia) para un contenido concreto, gestionar la distribución de ese contenido, y controlar lo que el consumidor puede hacer con ese contenido una vez que ha sido distribuido. (4)
Actualmente existen diferentes soluciones de DRM diseñadas por distintas empresas, pero en general todos tienen en común algunas características:

- Detectan quién accede a cada contenido, cuándo y bajo qué condiciones, y pueden reportar esta información al proveedor de la obra.
- Autorizan o deniegan de manera inapelable el acceso a la obra, de acuerdo a condiciones que pueden ser cambiadas unilateralmente por el proveedor de la obra con total independencia de lo que dicte el marco jurídico.
- Cuando autorizan el acceso, lo hacen bajo condiciones restrictivas que son fijadas unilateralmente por el proveedor de la obra, independientemente de los derechos que la ley otorgue al autor o al público.

Este documento pretende exponer diferentes tecnologías que pueden utilizarse en los sistemas DRM, además describir como pueden aplicarse en la esfera de la telefonía celular.

1.5. DRM en la telefonía celular.

Las tecnologías de descarga en teléfonos celulares han evolucionado desde la descarga de contenidos sencillos mediante SMS hasta las nuevas tecnologías que permiten descargar contenidos de una mayor calidad y de diferentes tipos. Con el objetivo de adaptarse a las tendencias y evolución del mercado, y poder soportar contenidos de una mayor calidad y atractivo para los usuarios, los operadores han ido ofreciendo tecnologías concretas que se orientan a la mensajería (SMS, MMS, etc.), las descargas WAP, las descargas de aplicaciones Java (WAP/HTTP), entre otras. Para ello se necesitan algunos procedimientos, como los ofrecidos por la tecnología DRM, que permitan regular y controlar el uso y la distribución de contenidos. Dentro de dichos procedimientos, es importante definir una serie de conceptos relacionados con la tecnología DRM.
Cuando se habla de contenido se refiere a un recurso digital, ya sea una imagen, conjunto de sonidos, entre otros, sobre los cuales se le asignan diferentes permisos y restricciones que definen su acceso, denominados Derechos de uso.

Los Derechos de uso están compuestos por permisos y restricciones que limitan el acceso al contenido, donde los permisos definen los tipos de operaciones que pueden realizarse sobre el contenido protegido (ejemplo visualización) mientras que las restricciones controlan el consumo de los contenidos; mediante las restricciones puede expresarse, por ejemplo, que una imagen sólo pueda ser visualizada un determinado número de veces.

Otro de los términos es el contenido DRM, el cual es el contenido que se consume de acuerdo a un conjunto de derechos, los que pueden estar incluidos en el propio contenido o se pueden descargar de forma independiente. Al hablar de mensaje DRM se hace referencia al mensaje que contiene el contenido DRM y opcionalmente, sus correspondientes derechos, este es el resultado final que se obtiene en el proceso de de protección de contenido. Pero este proceso no concluye al obtener el mensaje DRM ya que se debe garantizar una correcta aplicación de los derechos de uso al consumirse el contenido protegido, esta tarea la cumple el Agente DRM, entidad residente en el dispositivo consumidor.

La superdistribución es un procedimiento seguro que permite al usuario final redistribuir un contenido DRM a otros usuarios, a través de canales potencialmente inseguros. Por otro lado, también permite a los usuarios receptores adquirir los derechos de uso para el contenido DRM recibido.

Una solución DRM comprende un conjunto de acciones y procedimientos donde intervienen los conceptos antes expuestos permitiéndole a una entidad (operador o proveedor de contenidos) gestionar los derechos de acuerdo a los requisitos previamente establecidos. En el entorno móvil se dispone de diferentes tipos de soluciones, algunas de ellas propietarias y otras alineadas con estándares, ambos tipos de soluciones tienen el mismo objetivo, permitir una distribución controlada de los contenidos, con el fin de garantizar el cumplimiento de los derechos establecidos por las distintas partes (proveedor de contenidos, sociedades de autores, etc.) sobre un contenido digital.

Analizando la oferta actual de teléfonos móviles en el mercado, existen terminales que soportan tecnologías DRM “propietarias”, siendo estas tecnologías las siguientes:

- *On the phone preview* (desarrollada por Nokia, por ejemplo en su modelo Nokia 3410). Telefónica I+D está desarrollando actualmente un piloto sobre esta tecnología DRM.
- *Limited distributed* (desarrollada por Ericsson).

Por otra parte, el proveedor de tecnologías DRM, Intertrust Technologies, percibiendo este nuevo mercado ha desarrollado una nueva tecnología de DRM para la distribución de contenidos sobre redes inalámbricas hacia los dispositivos portátiles. Según la propia compañía, su sistema supone una gran ventaja tanto para los operadores como para los proveedores, ya que soporta múltiples tipos de clientes, y por tanto solamente se tiene que instalar una plataforma para dar servicio a todas las modalidades de cliente. Intertrust Technologies ha apostado fuerte por el desarrollo de una plataforma DRM para el sector de la telefonía móvil, estableciendo de hecho una alianza tecnológica con una potente compañía del sector como *Nokia*. A su vez, Nokia, líder mundial en la fabricación de teléfonos móviles, también tiene un acuerdo con la compañía IBM, sobre la distribución de contenidos digitales para aplicaciones y servicios móviles, según el cual IBM utiliza bajo licencia el software de servidor de Nokia para la descarga de contenido móvil.

Ambas empresas han acordado adoptar tecnologías DRM basándose en estándares abiertos y especificaciones comunes a toda la industria. En cuanto a las tecnologías alineadas a estándares no existe un estándar de la industria para los DRM y de hecho ésta es una de las discusiones que está dilatando y dificultando su implementación masiva.

1.6. Metodología DRM.

La estandarización de la tecnología DRM en el entorno móvil está actualmente liderada por OMA, Open Mobile Alliance. El proceso de estandarización tiene como objetivo homogeneizar los aspectos relacionados con el consumo controlado de contenidos digitales. Estos aspectos son:

- Permitir a los proveedores de contenidos expresar los derechos de uso sobre los contenidos digitales.
- Gestionar la previsualización de contenidos DRM.
- Evitar que los contenidos DRM sean distribuidos ilegalmente a otros usuarios.
- Permitir la superdistribución de contenidos DRM.
- Definir el procedimiento de autenticación de los agentes DRM.
- Definir mecanismos para el empaquetado y transferencia de derechos y contenidos protegidos.

Hasta el momento OMA ha definido 2 versiones de su metodología, 1.0 y 2.0.

OMA DRM V1.0

OMA Digital Rights Management V1.0 es la primera versión del estándar de protección de OMA y la más extendida por el momento con más de 400 modelos de teléfonos móviles que lo utilizan en todo el mundo. OMA DRM V1.0 se centra primordialmente en el control de copia y proporciona mecanismos básicos de gestión de las claves para desbloquear la copia de contenido. Los tres mecanismos de protección anti-copia definidos en esta versión son:

Bloqueo de envío (Forward Lock): Evita el envío de contenido a otro dispositivo deshabilitando las opciones de envío para el contenido protegido en el propio teléfono.

Distribución combinada (Combined Delivery): Se diferencia del mecanismo Forward Lock en cómo se gestiona el bloqueo. En este caso, el contenido se distribuye junto a los permisos y restricciones que tiene el contenido, los llamados Derechos de Uso.

Distribución separada (Separated Delivery). En este caso, el contenido se encripta generándose una clave de desbloqueo, la cual se distribuye separada del propio contenido junto a los derechos de uso, permitiendo ser utilizado como confirmación de la descarga.

Para los dos últimos mecanismos se requiere un servidor específico que gestione la emisión de la licencia de uso para cada descarga, normalmente se trata de una entidad independiente del propio servidor que gestiona la distribución de los contenidos.

OMA DRM V2.0.

OMA Digital Rights Management V2.0 hace especial hincapié en la seguridad de la protección, una de las principales carencias de la primera versión del estándar y realmente el impulsor de la nueva versión. Desde este punto de vista, OMA DRM V2.0 es una extensión de OMA DRM V1.0 pero con mayores medidas de seguridad y mejores mecanismos de cifrado.

OMA DRM V2.0 parte del modelo de Separated Delivery, añadiendo un sistema de cifrado de clave pública. Los dispositivos compatibles con OMA DRM V2.0 incluyen un certificado digital único con la clave pública que permite el envío cifrado del contenido y de la licencia de uso y sólo pueden ser descifrados por el dispositivo objetivo, que contiene el certificado digital adecuado con la clave pública para descifrar los objetos.

Como ventaja adicional de OMA DRM V2.0, la nueva versión ofrece mayor facilidad y flexibilidad a la hora de definir distintos modelos de licencia y distribución tales como

distribución viral, subscripciones o acceso por tiempo limitado; ya que elimina la dependencia del servidor para aplicar y comprobar los permisos cada vez que el usuario accede a un contenido protegido por OMA DRM V1.0. Esta versión de DRM ha sido aprobada no hace mucho tiempo y todavía está sufriendo numerosas modificaciones lo cual puede explicar el escaso apoyo obtenido hasta la fecha por parte de los fabricantes de teléfonos, que parecen estar esperando a que se estabilice el propio estándar antes de implementarlo. (1)

1.7. Arquitectura de las soluciones de DRM.

Atendiendo a su arquitectura, independientemente de que sean propietarias o alineadas con determinados estándares, las soluciones de DRM en el entorno móvil se pueden clasificar en dos grupos:

1. *El grupo de soluciones orientadas a un modelo cliente-servidor.*

La especificación OMA sobre DRM se encuentra dentro del modelo cliente-servidor. También existen otras soluciones propietarias, tanto en el entorno móvil como en el entorno fijo (Internet), que están basadas en este modelo.

Las soluciones de DRM orientadas a un modelo cliente-servidor disponen de un componente cliente y otro servidor, de manera que:

• El componente cliente, denominado agente DRM, reside en el dispositivo (terminal móvil, PDA, etc.) y se encarga de consumir el contenido en función de los derechos asociados. El cliente puede estar basado en múltiples tecnologías: hardware, software embebido en el dispositivo, aplicación de software asociada a un reproductor de contenidos, etc. El agente DRM sabe aplicar los derechos de uso establecidos sobre el contenido, como puede ser, por ejemplo, ejecutar un juego un número determinado de veces o escuchar una canción durante un periodo de tiempo concreto.

• El componente servidor, constituido por la *plataforma DRM*, contempla diferentes aspectos relacionados con la gestión de los derechos asociados a contenidos: el empaquetado de los contenidos y derechos, y la gestión de derechos.

2. *El grupo de soluciones orientadas a un modelo servidor (basadas en red)*.

Las soluciones de DRM orientadas a este modelo, en el entorno móvil, son generalmente propietarias. Estas soluciones se basan en la inclusión de marcas imperceptibles para los

usuarios, pero pueden ser detectadas por la solución alojada en la red del operador. Las principales características de estas soluciones son el marcado de contenidos (*watermarking*) y la detección de marcas. También sería posible definir algún grupo de soluciones mixto que incluyese características de las dos anteriores. El principal inconveniente de este grupo reside en la complejidad de la plataforma DRM, ya que debe cubrir la problemática existente en el modelo cliente-servidor (empaquetado, gestión de derechos, etc.) y en el modelo servidor (marcado de contenido).

Partiendo de los conceptos antes expuestos (metodología y arquitectura) se define para la solución del producto, utilizar la metodología propuesta por OMA, teniendo en cuenta que es el estándar a nivel mundial de la tecnología DRM en dispositivos móviles. De sus versiones, se aplicará la 1.0 debido a que es la versión base de la evolución de este estándar, recomendándose para futuras implementaciones el uso de versiones con mayor nivel de complejidad.

Como DRM va entrando en contacto cada vez con más aspectos de nuestras vidas cotidianas, es lógico que se alcen voces en contra. Algunos abogados especializados en propiedad intelectual y organizaciones de defensa al consumidor han empezado a preguntarse en voz alta si la DRM deposita demasiado control en las manos de las compañías de software. Y por otra parte, tal vez los proveedores de contenido multimedia no quieran esperar a que se organicen las ramificaciones legales de para aprovechar las ventajas de las nuevas tecnologías. (4)

1.8. Ventajas y desventajas.

La gestión de los derechos sobre bienes digitales en dispositivos móviles causa un efecto diferente sobre las entidades involucradas.

Desde el punto de vista del usuario, la gestión de derechos digitales presenta nuevos modelos de negocio que tienen implicaciones directas en la forma de consumir contenidos digitales. Mientras que los proveedores, podrán distribuir contenidos de valor añadido de una forma segura, con el objetivo de incrementar sus ingresos gracias a la distribución controlada que debe garantizar el operador. Como es de imaginar, la aplicación de DRM en diversos dispositivos ha causado controversia y más de alguna discusión entre quienes aprueban y rechazan este tipo de medidas. Los operadores suelen promocionarlo como algo realmente

útil para el usuario, aduciendo que la seguridad y confiabilidad de sus dispositivos e información se encuentran totalmente aseguradas, pero, con estos sistemas se puede generar un control de la conducta del usuario, sobre qué adquieren, preferencias o tasas de uso, por citar algunos, razón por lo que es rechazada por los usuarios, pues manifiestan que existe falta de privacidad, teniendo en cuenta que esto, puede ser muy peligroso en sistemas políticos autoritarios, pudiendo ser utilizada esta información para construir perfiles sobre sus preferencias informativas y venderlos con propósitos comerciales.

Mirándolo desde lado opuesto, los proveedores de los derechos pueden controlar, de forma segura, la explotación sucesiva de su obra, limitando los usos no autorizados y reduciendo la posibilidad de copias ilegales, además de una fuente de ingresos complementarios a las ventas. En fin, ayudarán a que aparezcan más y mejores contenidos digitales, al dificultar la difusión ilícita de la información; sin embargo, existe aún la imagen entre los titulares de que no son sistemas seguros y de que pueden ser fácilmente vulnerados y "craqueados".

En general, se puede afirmar que la aplicación de la tecnología DRM al entorno de las descargas en los dispositivos móviles potencia el negocio de la venta de contenidos digitales, gracias a una base tecnológica en la que se puedan apoyar los modelos de negocio. De cualquier modo, el diálogo es un buen síntoma de que va a ocurrir algo importante en el mundo celular con DRM. La crítica constructiva debería ser más que bienvenida en un mercado en el que la lucha por los derechos digitales acaba de empezar.

1.9. Tecnología.

Las tecnologías de DRM se basan principalmente en lenguajes de expresión de derechos y en los diversos aspectos de seguridad involucrados en DRM. Hay que hacer un énfasis especial en estos aspectos debido a que constituyen la base de las soluciones de DRM actuales, tanto en lo que respecta a las soluciones alineadas con determinados estándares como a las soluciones propietarias.

1.9.1. Lenguajes de expresión de derechos.

La tecnología del lenguaje de expresión de derechos se desarrolló inicialmente a principios de los años 1990 en el centro de investigación de Xerox en Palo Alto, California (Xerox Parc Research Center), Estados Unidos. Desde entonces, la tecnología ha alcanzado un creciente

grado de sofisticación. Esencialmente, se basa en la noción de que se otorga un permiso a un usuario para que éste realice un acto determinado relacionado con un contenido protegido por derechos de propiedad intelectual. Por ejemplo, si un titular de derechos desea otorgar a un usuario el derecho de copiar un determinado contenido para ser reproducido en el disco duro de una computadora, es posible otorgar dicho derecho con determinadas condiciones. El titular de derechos puede desear que se evite que el contenido pase a una tercera parte (es decir, que no sea copiado de nuevo) o que sea modificado de cualquier modo. Se trata de un permiso o autorización sencilla que una expresión de derechos puede formular como expresión de derechos legibles por una máquina.

Un lenguaje de expresión de derechos define la sintaxis y semántica de las reglas que gobiernan el uso de los derechos de un contenido protegido. Los principales objetivos de un lenguaje de expresión de derechos son los siguientes:

- Definir un mecanismo ligero y simple para la definición de los derechos.
- Disponer de un conjunto mínimo de permisos y restricciones.
- Realizar una implementación sencilla que permita una rápida salida al mercado.
- Facilitar la adopción de las tecnologías de DRM por parte de los proveedores de contenidos.
- Permitir especificar los derechos, independientemente del tipo de contenido, del medio de transporte y de que el contenido esté o no cifrado.
- Permitir definir pre-visualizaciones de contenidos.
- Definir restricciones sobre el número de veces que se puede acceder a un contenido, así como los límites temporales y los intervalos de acceso al contenido.

Para especificar los derechos sobre los contenidos, los lenguajes de expresión de derechos permiten definir modelos que agrupan conjuntos de derechos de acuerdo a su funcionalidad, permitiendo así la definición concisa de los derechos y de su semántica.

Para seleccionar uno u otro lenguaje hay que tener en cuenta la arquitectura y las necesidades concretas del sistema de DRM que se desea implantar.

Un lenguaje de expresión de derechos se escribe en algún tipo de lenguaje de computadora, probablemente XML. Este es un lenguaje de computadora de alto nivel que también puede ser leído (con algunas dificultades) por un ser humano. El lenguaje XML, a veces denominado el

lenguaje de la red, es ampliamente utilizado y su valor como lenguaje de expresión de derechos tiene la ventaja de su difusión, lo cual contribuye a la interoperabilidad.

Dentro de los lenguajes de expresión de derechos existentes se encuentra el desarrollado por Xerox de forma propietaria, el llamado DPRL (Digital Property Rights Language). Este lenguaje se utiliza principalmente para especificar diferentes derechos digitales de un mismo contenido. Se pueden imponer ciertas condiciones relacionadas con acceso, tarifa y tiempo para diferentes operaciones con el contenido digital (por ejemplo imprimir y copiar). Sin embargo este lenguaje no cumple criterios de integridad o de autenticación.

Los lenguajes mayoritariamente utilizados en soluciones DRM para móviles son versiones del XML. La más importante de ellas es el XrML (eXtensible rights Markup Language), que completa el lenguaje anterior de Xerox con una serie de estructuras y etiquetas semánticas con el fin de especificar los metadatos de un documento XrML, validando así la integridad de dichos documentos, así como el contenido digital.

Al igual que antes, existe la solución de carácter (código) abierto, ODRL (Open Digital Rights Language). Al ser de carácter abierto, no requiere ningún tipo de licencia, lo que puede suponer una ventaja para nuevos proveedores de servicio entrantes, como es el caso de la Plataforma de Gestión de Contenido. Este lenguaje también está basado en XML, es posible su uso en terminales móviles y lo más relevante es que el grupo de desarrollo OMA lo utiliza en la creación de sus productos.

Otro lenguaje es el XMCL (eXtensible Media Comerse Language), también de carácter abierto. Éste describe las reglas de uso de contenido multimedia, más bien basado en comercio móvil de contenidos digitales, sin embargo esta descripción es más simple que en los casos de XrML y ODRL. Este lenguaje, por el contrario, está muy indicado para arquitecturas DRM distribuidas. Estas tres últimas soluciones basadas en XML tienen diferentes puntos de vista, y la utilización de una u otra dependerá de la aplicación concreta que se le quiera dar.

Luego de una profunda investigación de los diferentes lenguajes de expresión de derechos se decide utilizar el ODRL debido a que al utilizarse la versión 1.0 de metodología desarrolla por OMA, la misma establece dentro de sus requisitos el uso de dicho lenguaje de expresión de derechos.

1.9.2. Seguridad.

La seguridad es un aspecto crucial de la tecnología DRM, ya que el principal objetivo de esta tecnología es ofrecer un canal seguro sobre el que se pueda realizar el uso y distribución de contenidos protegidos. Por tanto, la necesidad de confidencialidad en la información intercambiada es crítica.

Las tecnologías criptográficas.

En DRM las tecnologías criptográficas permiten identificar a los interlocutores involucrados en la distribución de un contenido DRM, evitando, además, que los usuarios no autorizados puedan acceder a contenidos protegidos o intenten suplantar a los usuarios autorizados.

Para proteger los contenidos del acceso no autorizado es necesario utilizar algún tipo de encriptación. La encriptación (cifrado), o proceso de hacer que la información no sea reconocible, se ha desarrollado durante miles de años. Se ha utilizado ampliamente en aplicaciones diplomáticas y militares, particularmente en tiempos de guerra para ocultar información al enemigo, aunque su utilización en el comercio es más reciente. Es ampliamente utilizada en el sector bancario y en otras áreas financieras vulnerables, en las que el intercambio y seguridad de las transacciones de información van siempre unidos.

El proceso de encriptación mediante dispositivos basados en microprocesadores para la gestión de derechos digitales implica la utilización de algoritmos (procedimientos matemáticos) para la protección de la información digital a fin de evitar que sea comprensible. De esta forma se puede proteger efectivamente del acceso no autorizado a la propiedad intelectual.

Independientemente de la esfera, en DRM se definen varios requisitos esenciales de la encriptación para que un sistema sea robusto con un nivel de seguridad suficiente que garantice que el contenido permanece seguro contra el acceso no autorizado o la manipulación.

- Seguridad suficiente: los sistemas de encriptación deben ser suficientemente seguros para el tipo de contenidos que desean proteger. Por ejemplo, es previsible que la publicación de un libro comercial necesite menos protección que un documento del gobierno que trate de secretos sobre armas nucleares. Debe existir un equilibrio entre el nivel de encriptación y la conveniencia del usuario.

- Conveniencia del usuario: los sistemas de encriptación no deben ser abusivos cuando el usuario deba utilizarlos. Por ejemplo, un sistema de encriptación que requiera que el usuario espere durante un periodo de tiempo que no sea razonable mientras que se ejecuta el proceso de seguridad, no es aceptable.
- Vulnerabilidad: Incluso los mejores sistemas de encriptación acaban siendo descifrados. Sin embargo, un sistema de encriptación debe diseñarse en la mayor medida posible de forma que una brecha en su seguridad no ponga en peligro la seguridad de todo el sistema, sino exclusivamente la de un dispositivo o identidad específica.

Si bien la utilización principal de la tecnología de encriptación es para que actúe de contenedor o como a menudo se denomina “envoltorio de contenidos” (“content wrapping”), también se utiliza para otras aplicaciones. Por ejemplo, la encriptación forma parte de la tecnología de firma digital, mediante la cual puede asegurarse el origen y la integridad del contenido e identidades. (3)

La metodología OMA propone la para las soluciones DRM la utilización del algoritmo Advanced Encryption Standard conocido también como Rijndael. Dentro de sus caracteristicas se encuentra que es inmune a los ataques conocidos, tiene un diseño simple, y puede ser implementado en la mayoría de los escenarios posibles, desde dispositivos con recursos limitados. (5)

1.10. Desarrollo del software.

1.10.1. Metodología RUP

El desarrollo de software nunca ha sido una tarea fácil, una prueba de ello es la gran cantidad de propuestas metodológicas para llevar a cabo un proyecto de software. Estas propuestas se encuentran divididas en dos grupos fundamentales: (CANÓS y otros).

• Las metodologías tradicionales o pesadas, las cuales se centran fundamentalmente en el control del proceso, estableciendo rigurosamente las actividades involucradas, los artefactos que se deben producir, y las herramientas y notaciones que se usarán.

• Las metodologías ágiles, las cuales se centran fundamentalmente en el factor humano y en el producto de software, dando mayor valor al individuo, a la colaboración con el cliente y al desarrollo incremental del software con iteraciones muy cortas.

Teniendo en cuenta que el proyecto de desarrollo de la Plataforma de Gestión de Contenido tiene una complejidad alta, que el equipo de trabajo supera a las 60 personas y que no cuenta con una amplia experiencia, es conveniente garantizar la calidad del proceso desde el principio y ganar en organización, por lo que se decide adoptar una metodología tradicional.

Se decide utilizar Rational Unified Process (RUP) como metodología de referencia para el desarrollo del software, por ser un proceso:

• Iterativo e incremental, lo cual permite dividir el proyecto en pequeños subproyectos para desarrollarlo en distintas etapas e iteraciones que resultan en un incremento del producto.

• Dirigido por Casos de Uso, el cual es uno de los métodos más utilizados y efectivos para reflejar los requisitos. Estos no solo sirven para especificar los requisitos, ellos son los encargados de guiar el ciclo de vida del proyecto.

• Centrado en la arquitectura, lo cual permite organizar o estructurar el sistema en sus partes más relevantes e ir refinando esta estructura progresivamente.

RUP define “un marco de trabajo genérico que puede especializarse para una gran variedad de sistemas software, para diferentes áreas de aplicación, diferentes tipos de organizaciones, diferentes niveles de aptitud y diferentes tamaños de proyecto”. (JACOBSON y otros 2004)

RUP propone flujos de trabajo en los que se definen las secuencias de actividades, quienes las deben desarrollar y los artefactos a generar. Entre estos flujos se encuentra el modelación del negocio donde se describen los procesos de negocio, identificando quienes participan y que actividades requieren automatización y requisitos que define qué es lo que el sistema debe hacer para lo cual se identifican las funcionalidades requeridas.

Utiliza el Leguaje Unificado de Modelado (Unified Modeling Lenguaje, UML), el cual los autores han seleccionado para visualizar, especificar y construir los artefactos del sistema automatizado a definir. (6)

1.11. Herramienta para el modelado visual.

Rational Rose es la herramienta CASE que comercializan los desarrolladores de UML y que soporta de forma completa la especificación del UML.

Esta herramienta propone la utilización de cuatro tipos de modelo (desarrollo iterativo, trabajo en grupo, generador de código e ingeniería inversa) para realizar un diseño del sistema, utilizando una vista estática y otra dinámica de los modelos del sistema, uno lógico y otro

físico. Permite crear y refinar estas vistas creando de esta forma un modelo completo que representa el dominio del problema y el sistema de software.

Rational Rose domina el mercado de herramientas para el análisis, modelado, diseño y construcción orientado a objetos.

De acuerdo a International Data Corporation (IDC), Por cuatro años consecutivos ha nombrado a Rational Rose como "La Herramienta Líder en Análisis, Diseño y Construcción Orientada a Objetos", con base en los ingresos del producto.

Los expertos de la industria, editores, y consumidores han honrado a Rational Rose con más premios que ninguna otra herramienta de modelado visual.

Rational es reconocido como el líder tecnológico por su rol en el desarrollo del UML, logrado en gran parte por los esfuerzos de Grady Booch, Ivar Jacobson, y Jim Rumbaugh, los tres más importantes autores del UML.

Rational Rose tiene todas las características que los desarrolladores, analistas, y arquitectos están exigiendo – soporte UML incomparable, completo soporte al equipo, desarrollo basado en componentes con soporte para arquitecturas líderes en la industria y modelos de componentes, facilidad de uso, integración optimizada, y mucho más. (6)

1.12. Lenguaje de programación.

1.12.1. Java.

Ofrece toda la funcionalidad de un lenguaje potente, pero sin las características menos usadas y más confusas de éstos, trabaja con sus datos como objetos y con interfaces a esos objetos. Soporta las tres características propias del paradigma de la orientación a objetos: encapsulación, herencia y polimorfismo.

Java se ha construido con extensas capacidades de interconexión TCP/IP, realiza verificaciones en busca de problemas tanto en tiempo de compilación como en tiempo de ejecución. La comprobación de tipos en Java ayuda a detectar errores, lo antes posible, en el ciclo de desarrollo.

Cuando se usa Java para crear un navegador, se combinan las características del lenguaje con protecciones de sentido común aplicadas al propio navegador.

Más allá de la portabilidad básica por ser de arquitectura independiente, Java implementa otros estándares de portabilidad para facilitar el desarrollo. Se beneficia todo lo posible de la tecnología orientada a objetos. Java no intenta conectar todos los módulos que comprenden una aplicación hasta el tiempo de ejecución.

1.13. IDE

1.13.1. Eclipse IDE 3.3

SE propone utilizar esta herramienta para la futura implementación ya que es un editor visual con sintaxis coloreada, compilación incremental de código, modifica e inspecciona valores de variables, avisa de los errores cometidos mediante una ventana secundaria, depura código que resida en una máquina remota.

1.14. Conclusiones del capítulo.

Se ha hecho mención de los principales conceptos que se abordaran a lo largo de todo este trabajo, introduciendo al lector en la terminología utilizada en el campo de la administración de derechos digitales para móviles. Se profundizó el las soluciones alternativas que existen en el mercado internacional, así como, algunas de sus ventajas y las principales desventajas que influyen directamente en el problema a resolver. Además, se abordaron las herramientas y la metodología de desarrollo para la construcción de la solución.

Capítulo 2

Características del sistema

2.1 Introducción.

En el capítulo se hará la descripción de la propuesta del trabajo, para lo que se determinarán los procesos de negocio que tienen que ver con el campo de acción, en base a lo cual se conformará un modelo de dominio. Además se enumerarán los requisitos funcionales y no funcionales que debe tener el sistema en proposición; se identificarán los Casos de Uso y finalmente se hará la propuesta de las funcionalidades del producto mediante el diagrama Casos de Uso del sistema (CUs).

2.2 Descripción del sistema propuesto.

Para describir las funcionalidades que se deben desarrollar en el sistema es necesario enfocarse en las características que identifican a los tres algoritmos representados por la metodología de Administración de Derechos Digitales para la protección de contenidos, estos son: Forward Lock, Combined Delivery y Separated Delivery.

Dichos métodos tienen en común la creación de un mensaje DRM, teniendo en cuenta de que en los tres se realiza de manera diferente, este mensaje tiene la estructura de un mensaje multipartes.

Los mensajes multipartes (multi-part), presentan uno o más conjuntos diferentes de datos de forma combinada en un cuerpo único. El formato de los mensajes de múltiples partes se define basado en las Extensiones Multipropósito al Correo de Internet (Multipurpose Internet Mail Extensions [MIME]), las cuales son una serie de convenciones o especificaciones dirigidas al intercambio a través de Internet todo tipo de archivos (texto, audio, vídeo, etc.) de forma transparente para el usuario. (7)

En el método Forward Lock el mensaje DRM estará compuesto por una sola parte, relacionada exclusivamente con el contenido multimedia convertido a flujo de datos.

Los algoritmos Combined Delivery y Separated Delivery además del mensaje DRM, tienen en común la creación de los Derechos de Uso donde se analizan diversos aspectos con los que se conformará un XML, pero en ambos métodos se generan de diferentes formas; uno de los aspectos a tener en cuenta son los permisos de ejecución sobre el contenido multimedia, a continuación se definen:

Tipo de contenido	**Permisos**
Música o Video	*Play*
Aplicaciones Java, ejemplo juegos	*Execute*
Imágenes	*Display*

Tabla 1.

Estos permisos tienen asociadas diferentes restricciones las cuales limitan las operaciones que pueden ejecutarse en el teléfono sobre el contenido protegido, que es otro de los aspectos a tener en cuenta par la creación de los Derechos de Uso.

Las restricciones son definidas por el proveedor del contenido a proteger, acción que se administra en el Módulo de Contenido de la Plataforma de Gestión de contenido para dispositivos móviles. Existen diferentes tipos de restricciones, una de ellas son las de tiempo, pudiendo estar definidas en un rango donde se especifica el momento en que se comienza y en el que se termina; o descritas en un valor durante el cual se puede ejecutar esa acción. También se definen las veces que se puede ejecutar el contenido restringiendo la cantidad de ejecuciones que se pueden realizar sobre el mismo.

Finalmente como parte del proceso de la creación de los Derechos de Uso, se genera un identificador que describe el momento exacto en el que se protege el contenido, es responsabilidad de los desarrolladores garantizar que este identificador sea único.

En el método Combined Delivery al obtener los Derechos de Uso, los mismos pasarán a formar parte del cuerpo del mensaje DRM junto al contenido convertido en flujo de datos.

El proceso de protección de contenido mediante el uso del algoritmo Separated Delivery es el más complejo de los tres, pero a su vez, el más seguro. Una de las características que lo ilustra es el uso del método de encriptación simétrico Advanced Encryption Standard (AES). Al aplicar el AES se obtendrá la llave de decodificación Content Encryption Key (CEK), la cual

formará parte de los Derechos de Uso, este campo es el que marca la diferencia entre los Derechos de Uso generados en el método Combined Delivery y los generado por el Separated Delivery.

OMA DRM en el método Separated Delivery define la creación del DRM Content Format (DCF). Los DCF al igual que los mensajes DRM, son mensajes multipartes donde se empaqueta el contenido cifrado junto diferentes metadatos:

- Información del contenido multimedia original, tales como su nombre, una breve descripción y el nombre de su proveedor.
- El identificador de los Derechos de Uso.
- Información acerca de los detalles de encriptación.
- Dirección donde se publicarán los Derechos de Uso.

Luego de crear el DCF este formará parte del mensaje DRM. Es importante señalar que sin la presencia en el teléfono del XML que describe los Derechos de Uso, sería imposible abrir el contenido encriptado que contiene el mensaje DRM, ya que en este XML está la CEK que es la llave para desencriptar dicho contenido.

Otro de los procesos que se realiza en este método es la codificación del XML de los Derechos de Uso, la creación del WAP Binary XML (WBXML).

WBXML ha sido desarrollado por la Open Mobile Alliance como un estándar para permitir que los documentos XML sean transmitidos de un manera compacta a través de la redes de telefonía móvil y fue propuesto como una de las familias de estándares del World Wide Web Consortium's Wireless Application Protocol.

En resumen, el sistema permitirá gestionar la protección del contenido digital, mediante la aplicación de los algoritmos que propone la metodología OMA DRM 1.0.

2.3 Modelado de dominio.

El hecho de que los procesos del negocio tengan muy bajo nivel de estructuración; que sea difícil el establecimiento de reglas para la gestión como tal de los artefactos que se vayan definiendo en el proceso de desarrollo; que no existan flujos de información interconectados y bien definidos; inciden en que no se pueda llevar a cabo un modelado de negocio, haciéndose

necesario uno de dominio. A continuación se representa el diagrama del Modelo de Dominio partiendo de los conceptos involucrados en la lógica de los algoritmos para la protección de contenido:

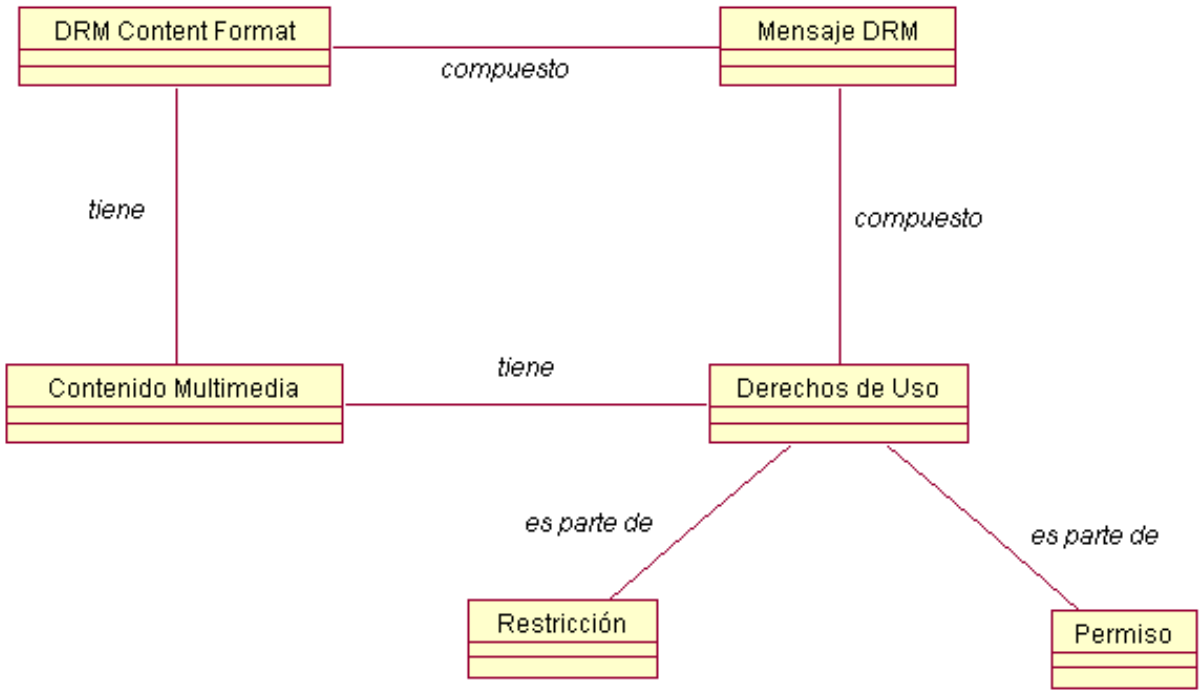

Figura 1. Modelo del Dominio.

2.4 Requerimientos funcionales.

De acuerdo con los objetivos planteados, el sistema debe ser capaz de:

RF1. Protección de contenido.
1.1. Analizar las capabilities DRM.
1.2. Determinar el método para la protección del contenido según la jerarquía que existe.

RF2. Método Forward Lock.
2.1Aplicar el método Forward Lock para proteger el contenido.

RF3. Método Combined Delivery.
3.1 Aplicar el método Combined Delivery para proteger el contenido.

RF4. Método Separated Delivery.
4.1 Aplicar el método Separated Delivery para proteger el contenido.

RF5. Solicitar la entrega.

Solicitar la entrega del contenido al Módulo de descarga.

2.5 Requerimientos no funcionales.

Los requisitos no funcionales son las propiedades o cualidades que el producto debe tener y que lo hacen atractivo, usable, rápido o confiable. A continuación se listan los que corresponden al sistema en proposición.

Usabilidad

- El módulo solo podrá ser usado por los desarrolladores de la plataforma.

Seguridad

- Proteger contra acciones no autorizadas o que puedan afectar la integridad de los datos.
- Emplear los métodos de encriptación para garantizar el correcto funcionamiento de la metodología DRM.

Confiabilidad

- El sistema debe ser capaz de recuperarse ante la ocurrencia de un fallo, de no ser posible, emitir alertas al personal encargado de la administración del mismo, así como proteger la información y contenidos.

Fiabilidad

Realización de mantenimientos preventivos.

- No existe la necesidad de efectuar mantenimientos preventivos que afecten la vitalidad del sistema, estos procesos deberán realizarse en tiempo de ejecución.

Eficiencia

- Tiempo de respuesta por transacciones.
- Los tiempos de respuesta serán reducidos al máximo.
- Rendimiento: el 95% de las transacciones deben de realizarse en menos de un segundo.
- Capacidad: el sistema debe de permitir que estén conectadas como mínimos 400 personas al mismo tiempo.

Soporte

La UCI brindará soporte.

- La UCI debe brindar soporte tanto a administradores que necesiten un breve entrenamiento para operar el sistema, puede ser mantenimiento, entrenamiento de personal u operar directamente el sistema.

Portabilidad

- Necesidad de que el sistema sea multiplataforma.

2.6 Modelo de Casos de Uso.

Para desarrollar el modelo de CU es necesario determinar el actor y los CU que se plasmarán en él.

Tabla 2. Descripción del Actor del sistema.

Actor	Justificación
Módulo de Descarga.	Es un módulo de la Plataforma de Gestión de Contenido encargado de administrar las descargar que se realizan. Cuando un usuario solicite la descargar de contenido, este pasará dicho contenido hacia el Módulo de Administración de Derechos Digitales donde se efectuará su protección.

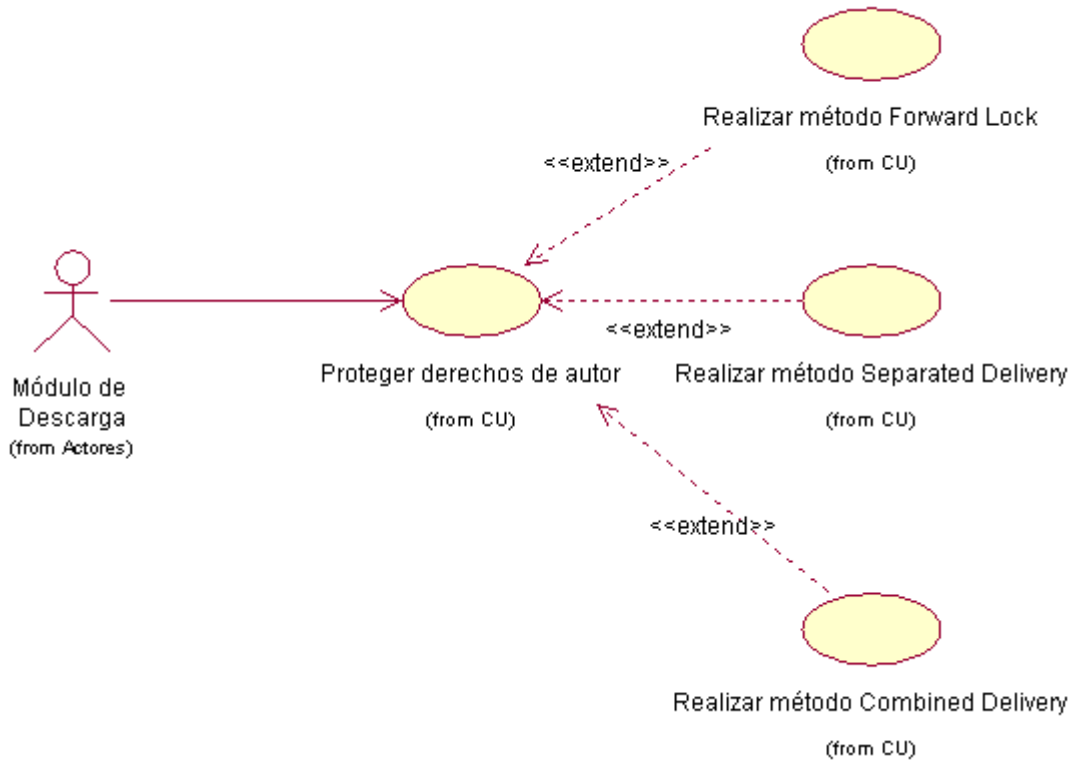

Figura 2. Diagrama Casos de Uso del Sistema.

La propuesta del presente trabajo tiene 4 Casos de Uso del sistema que engloban los 5 requisitos funcionales. En el epígrafe siguiente se describen cada uno de ellos.

2.7 Determinación de los Casos de Uso.

Tabla 3- CU Gestionar información.

CU-1	**Protección de contenido.**
Actor	Módulo de Descarga.
Descripción	El caso de uso se inicia cuando el sistema recibe el User Agent que identifica al teléfono que hace la solicitud de descarga, luego accede a las capabilities DRM para analizar los métodos de protección de contenido que soporta el teléfono mediante la información que brinda el User Agent y finaliza determinando qué método utilizar en dependencia de la jerarquía de los mismos.
Referencia	**RF 1**

Tabla 4- CU Método Forward Lock.

CU-2	**Método Forward Lock**.
Actor	Módulo de Descarga.
Descripción	El caso de uso comienza cuando el sistema al haber determinado este algoritmo DRM a aplicar, recibe el contenido a proteger para luego armar el mensaje DRM y realizar la solicitud de su entrega.
Referencia	**RF2, RF5**

Tabla 5- CU Método Combined Delivery.

CU-3	**Método Combined Delivery**
Actor	Módulo de Descarga de Contenido.
Descripción	El caso de uso comienza cuando el sistema al haber determinado este algoritmo DRM, recibe el contenido a proteger generando los Derechos de Uso a partir de las restricciones asociadas al contenido y finaliza obteniéndose el empaquetado del contenido en el mensaje DRM junto a los Derechos de Uso, para luego realizar, la solicitud de su entrega.
Referencia	**RF3, RF5**

Tabla 6 - CU Método Separated Delivery.

CU-4	**Método Separated Delivery.**
Actor	Módulo de Descarga
Descripción	El caso de uso comienza cuando el sistema al haber determinado este algoritmo DRM, recibe el contenido a proteger encriptando así el contenido y luego armar el mensaje DRM y los Derechos de Uso finaliza obteniéndose al realizar la solicitud de su entrega de los Derechos de Uso y del mensaje DRM por separado.
Referencia	**RF4, RF5**

2.8 Conclusiones del capítulo.

Este capítulo fue el comienzo del desarrollo de la propuesta de solución que se obtuvo a partir del análisis de los procesos del negocio, de los requisitos que debe cumplir el sistema, agrupados en CUs y que se representaron finalmente en un diagrama de CU, la base del futuro sistema.

Capítulo 3

Análisis y diseño del sistema

3.1 Introducción

El capítulo tiene como objetivo principal realizar el modelo de análisis y diseño, efectuando la realización de los Casos de Uso mediante los diagramas de colaboración del análisis, además se desarrolla el diagrama de clases del diseño teniendo en cuenta los patrones que han sido resultado de prácticas de diseñadores expertos en orientación a objetos, lo cual permite que el producto sea escalable, reutilizable y flexible; finalmente se modelan loa diagramas de secuencia de diseño. Este flujo de trabajo tiene una gran importancia en el ciclo de desarrollo pues traduce los requisitos definidos a funcionalidades que debe realizar el producto, obteniéndose como resultado el modelo de diseño que es una entrada principal para la disciplina de la futura implementación.

3.2 Modelo de Análisis.

El modelo de análisis ayuda a refinar los requisitos y permite razonar sobre los aspectos internos del sistema, no se toma en cuenta el lenguaje de programación a usar en la construcción, ni la plataforma en la que se ejecutará la aplicación, entre otras características que afectan al sistema, ya que el objetivo del análisis es comprender perfectamente los requisitos del software y no precisar cómo se implementará. Puede considerarse como una primera aproximación al modelo de diseño, y es por tanto, una entrada fundamental cuando se da forma al sistema en el diseño y la implementación.

3.3 Diagramas de Clases del Análisis.

Un diagrama de clases del análisis representa una abstracción de una o varias clases y/o subsistemas del diseño del sistema. Describe gráficamente las especificaciones de las clases de software, de las interfaces, así como sus relaciones en una aplicación.

Por su parte, una clase del análisis representa una abstracción de una o varias clases del diseño del sistema y siempre encajan en uno de tres estereotipos básicos: interfaz, control o entidad.

Las clases interfaz son las que modelan la interacción entre el sistema y sus actores, mostrando un entorno amigable para el usuario. El módulo en desarrollo no presenta este tipo de clases del análisis, pues, en ningún momento existe interacción con el usuario final mediante una interfaz gráfica, debido a que son procesos que se generan de forma automática.

Las clases controladoras (control) coordinan el trabajo de los Casos de Uso, así como las actividades de los objetos que implementan la funcionalidad del caso de uso, por lo que definen el flujo de control y las transacciones dentro de un caso de uso. En el proceso del análisis se identificaron diferentes clases controladoras (CC_DRMControl, CC_WURFL, CC_Forward Lock, CC_Combined Delivery, CC_Separated Delivery)

Además se encuentran las clases entidad, donde se modela información que posee una larga vida y que a menudo es persistente; así como fenómenos, conceptos y sucesos que ocurren en el mundo real. Como parte del proceso de investigación y análisis de la metodología DRM se identificaron 6 clases entidad (CE_Content, CE_Permission, CE_Time, CE_CountExecution, CE_Interval, CE_DataTime).

A continuación se muestran el diagrama general de clases del análisis, donde se representan los Casos de Uso del sistema descritos en el documento.

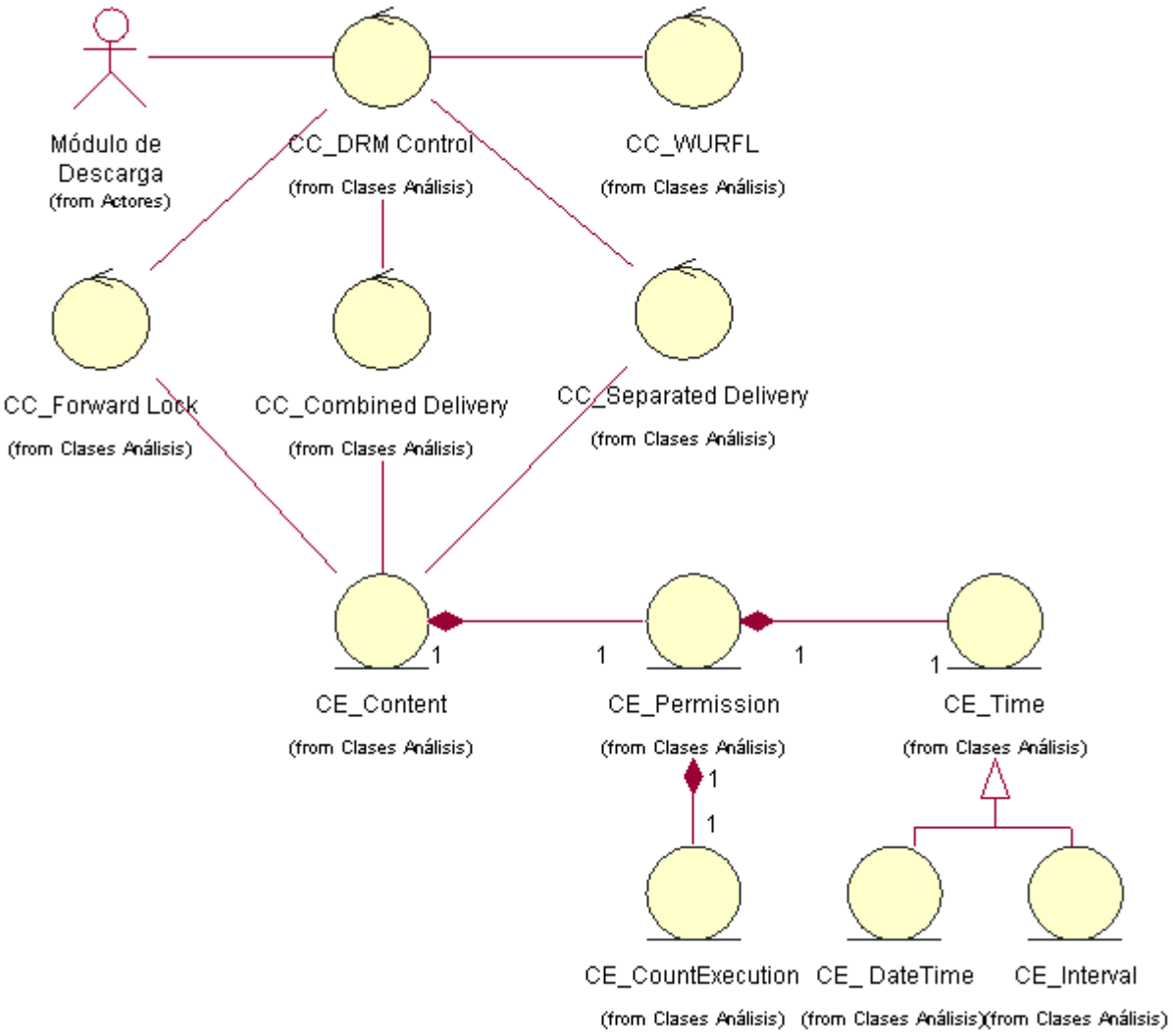

Figura 3. Diagrama de general clases de análisis.

3.4 Diagramas de Colaboración.

La secuencia de acciones en un caso de uso comienza cuando un actor invoca el caso de uso mediante el envío de algún tipo de mensaje al sistema. En el análisis se utilizaron los diagramas de colaboración pues el objetivo fundamental es identificar requisitos y responsabilidades sobre los objetos, y no de identificar la secuencia de interacción detalladas y ordenadas cronológicamente (en el diseño se utilizarán los diagramas de secuencia). (8)

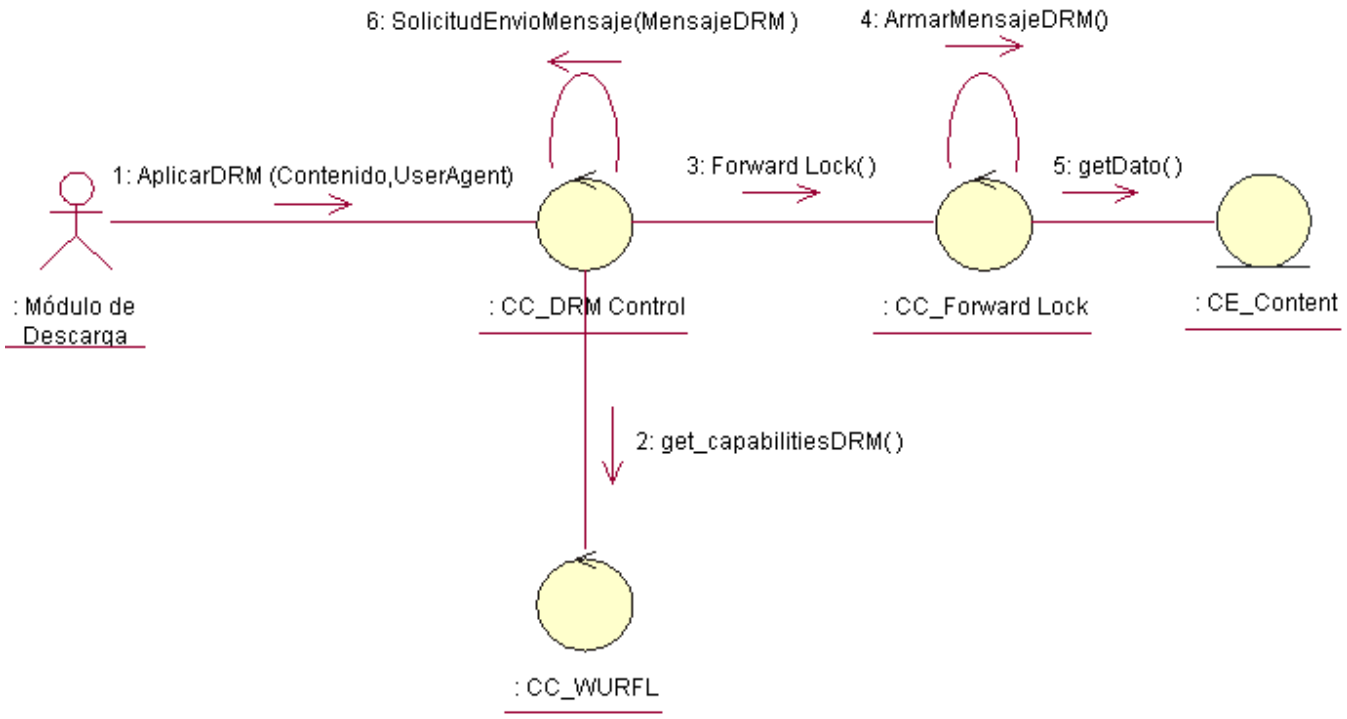

Figura 4. Diagrama de colaboración CU: Forward Lock**.**

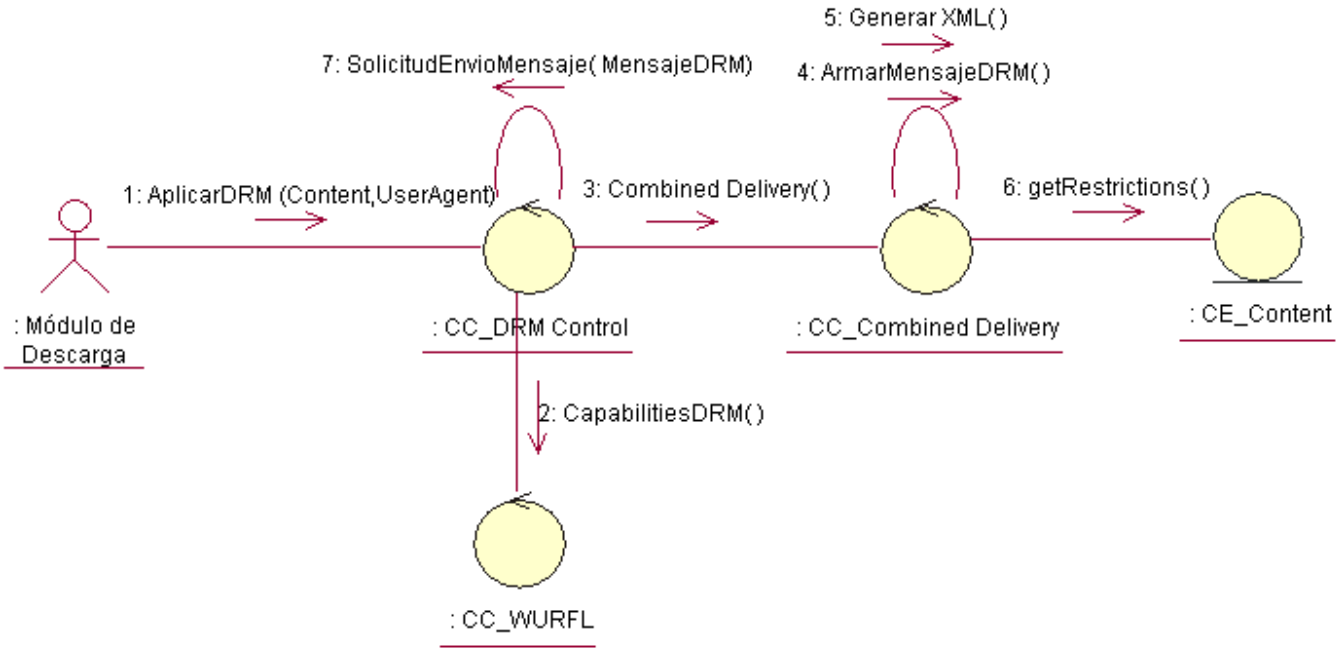

Figura 5. Diagrama de colaboración CU: Combined Delivery.

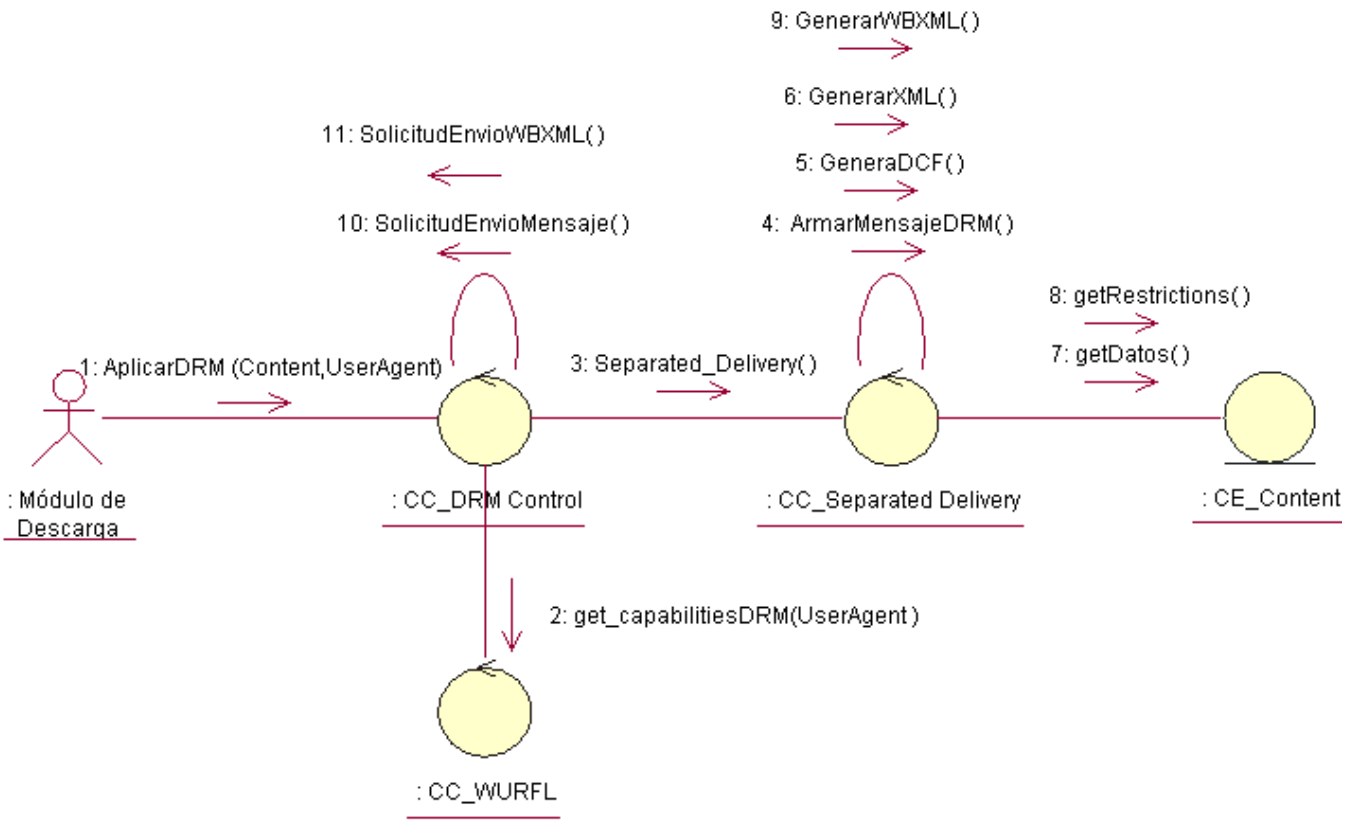

Figura 6. Diagrama de colaboración CU: Separated Delivery.

3.5 Modelo de diseño.

El desarrollo del software es una tarea complicada que depende en gran medida de la experiencia de las personas involucradas, por lo que la comprensión del software es el pilar que sustenta un correcto diseño correspondiente. Los mecanismos de reutilización son los recursos más utilizados para el diseño, que al ser experiencias de diseñadores expertos en orientación a objetos; permiten dar solución a problemas mediante la codificación del conocimiento y principios existentes, facilitando notablemente el trabajo posterior.

Con la reutilización se consigue:

- Reducción de tiempos.
- Disminución del esfuerzo de mantenimiento.

- Eficiencia.
- Consistencia.
- Fiabilidad.
- Protección de la inversión en desarrollos.

Entre los mecanismos de reutilización más utilizados se encuentran los patrones.

3.6 Patrones

Los patrones se pueden definir como una solución a un problema en un contexto, son teorías genéricas. Se basan en la experiencia acumulada por los que resuelven problemas reiterativos.

"Cada patrón describe un problema que ocurre una y otra vez en nuestro ambiente, y luego describe el núcleo de la solución a ese problema, de tal manera que puede usar esa solución un millón de veces más, sin hacer jamás la misma cosa dos veces."(9)

Existen diferentes clasificaciones. Dentro de los patrones de producto de software se encuentran los de análisis, arquitectura, diseño y lenguaje de programación. Para el desarrollo de la solución se aplicaron diferentes patrones de diseño, fundamentalmente los patrones de diseño: GRASP y GoF, con el objetivo de facilitar el mantenimiento del software y contribuir a la realización de un producto reutilizable y escalable. (10)

3.6.1 Patrones GRASP

Los patrones de asignación de responsabilidades GRASP (*del inglés: General Responsibility Assignment Software Patterns*), permiten asignar correctamente las responsabilidades a cada una de las clases que intervienen en el modelo; fueron tomados en cuenta para el diseño de clases y métodos de cada una de ellas. Se utilizaron seis de los nueve patrones GRASP: (11)

- Controlador. (Controller): Encargado de manejar los eventos del sistema que representan la visión general del sistema o de un caso de uso, por ejemplo: toda la lógica del sistema se dirige en la clase DRMControl.

- Experto. Describe la asignación responsabilidades al experto en información; la clase que posee la información necesaria para cumplir con la responsabilidad, por ejemplo: la clase WURFL es la especialista en el manejo de todas las características (capabilities) del teléfono que realiza la solicitud de descarga, es la que brindará la información de cuál método DRM se utilizará para proteger el contenido.

- Creador: Se refiere a asignar responsabilidades a las clases de crear instancias de otras conociendo que las primeras son las que contienen la información para ello, por ejemplo: la clase Permission le brinda a la clase Content un objeto de tipo Time, por tanto Permission es la idónea para crear una instancia de Time.

- Polimorfismo. Cuando varía el tipo (clase) de alternativas o comportamientos relacionados, asignar la responsabilidad del comportamiento -mediante operaciones polimórficas- a los tipos en que varía el comportamiento, por ejemplo la clase DRMProtection, tiene como clases hijas (ForwardLock, CombinedDelivery y SeparatedDelivery) donde se redefine la funcionalidad (método) MensajeDRM() ya que se realiza esta operación de forma diferente en cada una.

- Bajo acoplamiento. Cada clase está acoplada (relacionada) a las clases estrictamente necesarias, garantizando un bajo impacto de los cambios que se producen en una clase para las demás clases que se relacionan con ella, por ejemplo: la clase Permission, no conoce la existencia de la clase DRMProtection, ya que no es necesario.

- Alta cohesión. Asignar responsabilidades a las clases de manera que todos sus métodos tuvieran un comportamiento bien definido, este patrón se aplica en todas las clases del diseño ya que en cada una, solo se implementan las funcionalidades que le corresponden.

Otro conjunto de patrones bien conocidos son los patrones de la pandilla de los cuatro GoF (*del inglés: Gang of Four*) se dividen en 3 grupos fundamentales: creacionales, estructurales y de comportamiento. Uno de estos fueron aplicados directamente en el diseño de este sistema,

a continuación se menciona el nombre del patrón y las clases donde se aplicaron directamente.

3.6.2 Patrones GoF

En el diseño de clases se utilizaron los patrones de creación, estos muestran la guía de cómo crear objetos cuando sus creaciones requieren tomar decisiones. Estas decisiones normalmente serán resueltas dinámicamente decidiendo que clases instanciar o sobre que objetos un objeto delegará responsabilidades.

- Método Factoría (Factory Method): Define una interfaz para la creación de un objeto, pero permitiendo a las subclases decidir de que clase instanciarlo. Permite, por tanto, que una clase difiera la instanciación en favor de sus subclases. Este patrón de pone de manifiesto en las clases DRMFactory, CreatorFL, CreatorCD, CreatorSD.

En los epígrafes siguientes se describirán: (1) el diagrama de clases de diseño, que muestra las clases y sus interrelaciones, dando una idea de los elementos participantes en la realización de cada CU, (2) la descripción de las clases que interactúan en el diagrama de clases del diseño, detallando sus funcionalidades y finalmente (3) los diagramas de secuencia del diseño donde se identifican la interacción entre los objetos ordenadas cronológicamente.

3.7 Diagrama de clases del diseño

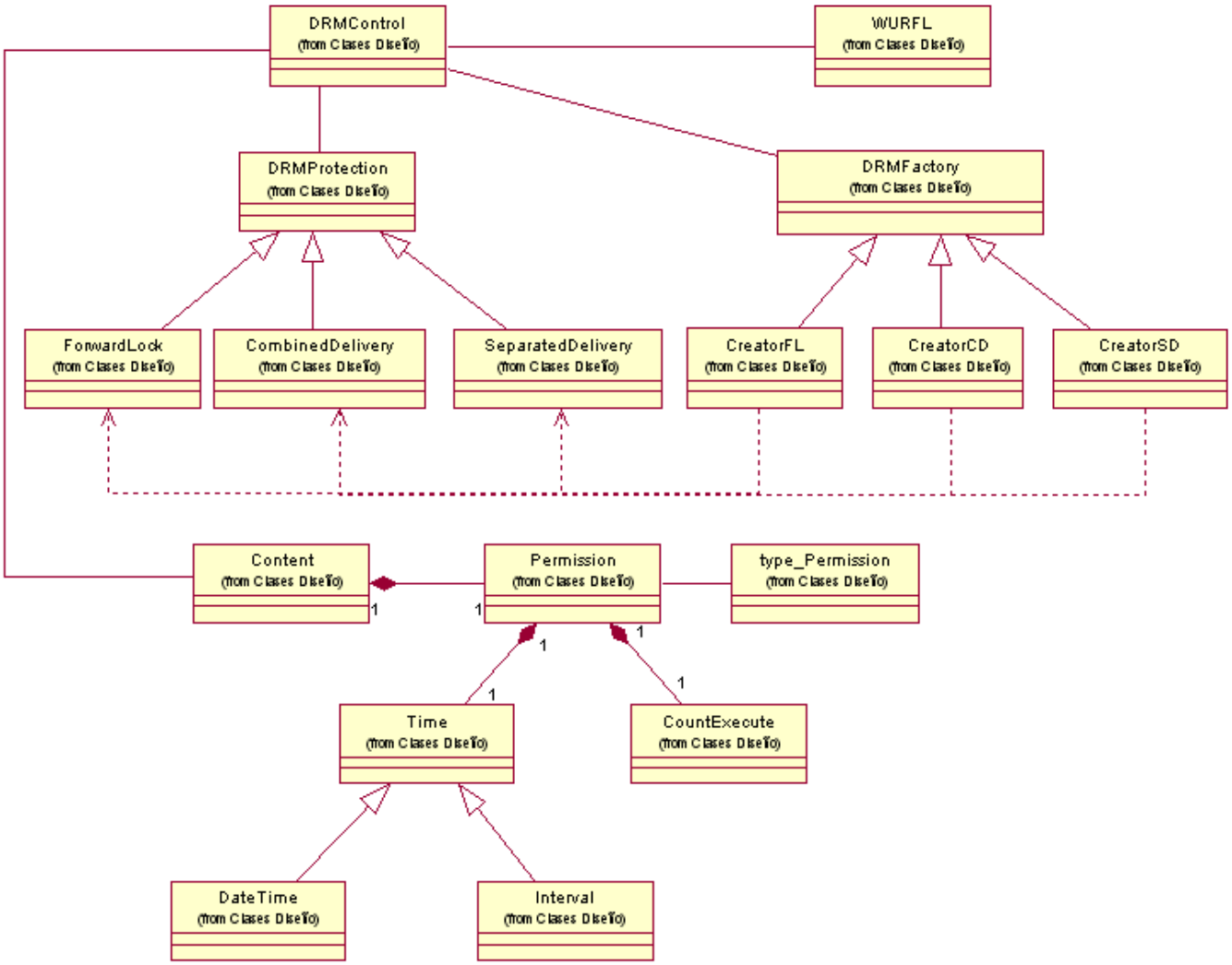

Figura 7. Diagrama de clases de diseño.

3.8 Descripción de las clases del diseño.

Las clases del diseño se definen en dependencia del lenguaje de programación, consecuentemente las operaciones, parámetros, atributos, tipos y demás, son especificados utilizando la sintaxis del lenguaje de programación elegido, en este caso se utilizará Java. (8)

Entre las diferentes clases identificadas, es necesario reflexionar sobre el funcionamiento de la clase WURFL.(12) Una clase de este tipo, especifica cada una de las características de los dispositivos inalámbricos, ya sean móviles, PDA, etc. Proporciona información sobre su

configuración, características y funcionamiento, por ejemplo: características generales del dispositivo (ej. modelo, marca); capacidad de procesamiento de imágenes (soporte para gif, flash lite, colores de pantalla). A partir de la información que brindará esta clase se definirá qué algoritmo DRM se utilizará para la protección del contenido.

Tabla 7- Clase DRMControl.

Método	**Descripción**
DeterminateMethod(UserAgent): String	A partir del UserAgent se analiza qué método DRM soporta el teléfono que realiza la solicitud y se determina cuál de estos métodos se utilizará para la protección del contenido teniendo en cuenta su jerarquía (Separated Delivery, Combined Delivery, Forward Lock).
Protection(Content): byte[]	Se protege el contenido mediante un método DRM.
ResponseMessage(DRMMessage):byte[]	Realiza la solicitud de entrega del mensaje DRM.
ResponseWBXML(WBXML): byte []	Realiza la solicitud de los Derechos de Uso en formato comprimido.

Tabla 8- Clase WURFL.

Método	**Descripción**
getCapabilitiesDRM: CapabilitiesDRM	Retorna un objeto de tipo Capabilities donde se especifican las capabilities DRM del teléfono que realiza la solicitud de descarga.

Tabla 9- Clase DRMProtection.

Método	**Descripción**

DRMMessage(): byte[]	Es un método puro de esta clase padre que se encarga de armar el mensaje DRM, redefinido en cada clase hija debido a que cada algoritmo DRM genera el mensaje de forma diferente.

Tabla 10- Clase ForwardLock.

Método	**Descripción**
DRMMessage(Content): byte[]	Arma el mensaje DRM el cual está compuesto por el contenido convertido a flujo de bytes.
ConvertContent(Content):byte[]	Convierte el contenido a un flujo de bytes.

Tabla 11- Clase CombinedDelivery.

Método	**Descripción**
DRMMessage(Content): byte[]	Arma el mensaje DRM teniendo en cuenta que su cuerpo esta compuesto por el XML de los Derechos de Uso y el contenido convertido en flujo de bytes. Ver anexo Mensaje DRM.
GenerateXML(Content): XML	Crea los Derechos de Uso en formato de XML, el cual está compuesto por la acción que se puede ejecutar sobre el contenido y las restricciones asociadas las cuales son definidas por el proveedor del contenido. Ver anexo Derechos de Uso.
GenerateID(): int	Genera un identificador único que describe el momento exacto en el que se protege el contenido, este identificador forma parte del

	XML de los Derechos de Uso.
ConvertContent(Content):byte[]	Convierte el contenido a un flujo de bytes.

Tabla 12- Clase SeparatedDelivery.

Método	**Descripción**
DRMMessage(Content): byte[]	Arma el mensaje DRM; este mensaje está compuesto por el contenido encriptado y toda la información asociada a este, es decir está compuesto por el mensaje DCF.
AES(Content): String CEK	Encripta el contenido mediante el método de encriptación simétrico Advanced Encryption Standard.
GenerateDCF(Content): byte[]	Genera el mensaje DCF luego de encriptar el contenido.
GenerateXML(Content):byte[]	Crea el XML, el cual está formado por la acción que se puede ejecutar sobre el contenido y las restricciones asociadas.
GenerateWBXML():byte[]	Comprime el XML de los Derechos de Uso.
ConvertContent(Content):byte[]	Convierte el contenido a un flujo de bytes.

Tabla 13- Nomenclador type_Permission.

Atributos	**Descripción**
Id	Identificador del nomenclador.
Descripción	Describe los tipos de acciones que se pueden ejecutar sobre el contenido, por ejemplo: play, execute, display.

3.9 Diagramas de Secuencia

Mediante estos diagramas se muestra la secuencia de mensajes entre objetos durante un escenario concreto resaltando la ordenación temporal de los mensajes que se intercambian. (13)

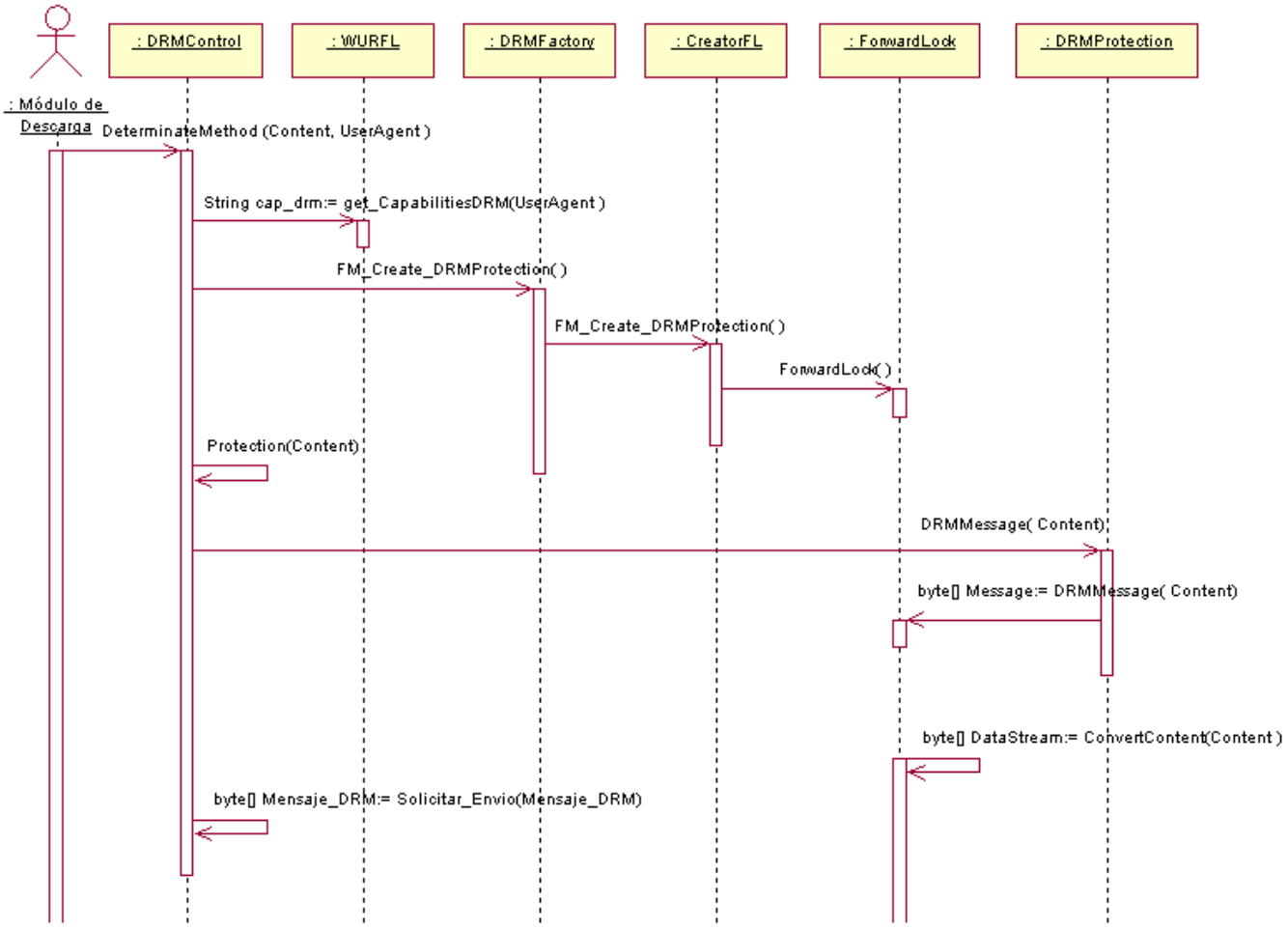

Figura 8. Diagrama de secuencia CU: Forward Lock.

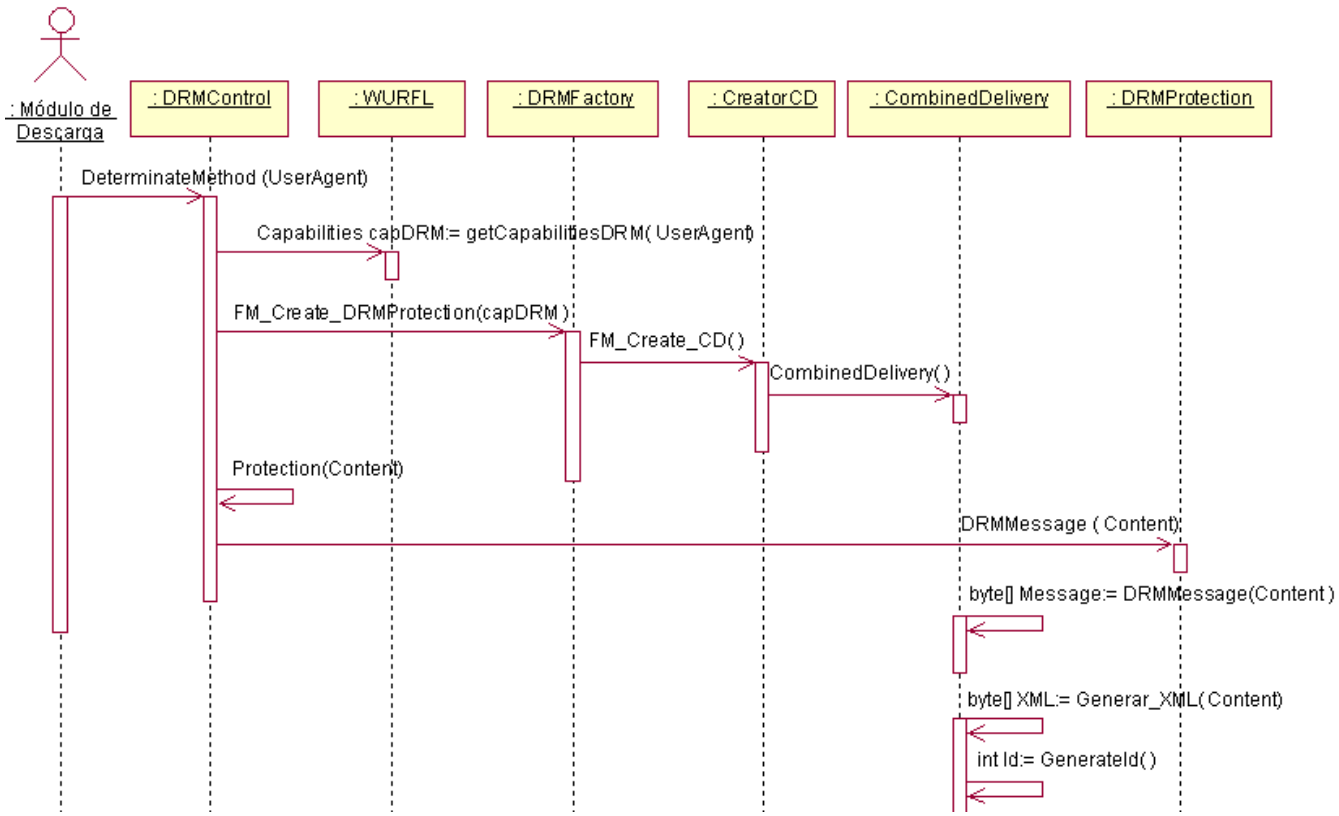

Figura 9a. Diagrama de secuencia CU: Combined Delivery.

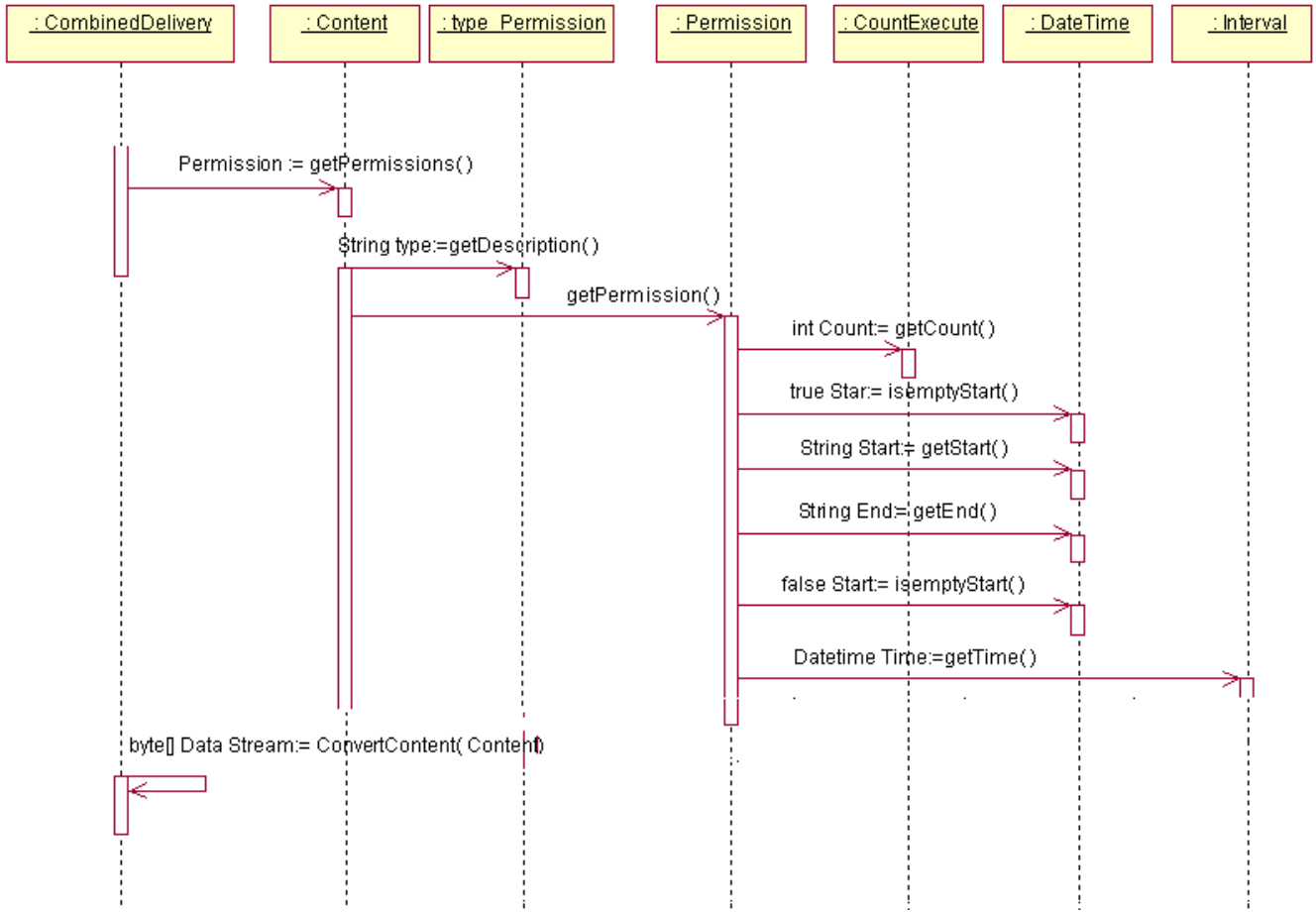

Figura 9b. Continuación del Diagrama de secuencia CU: Combined Delivery.

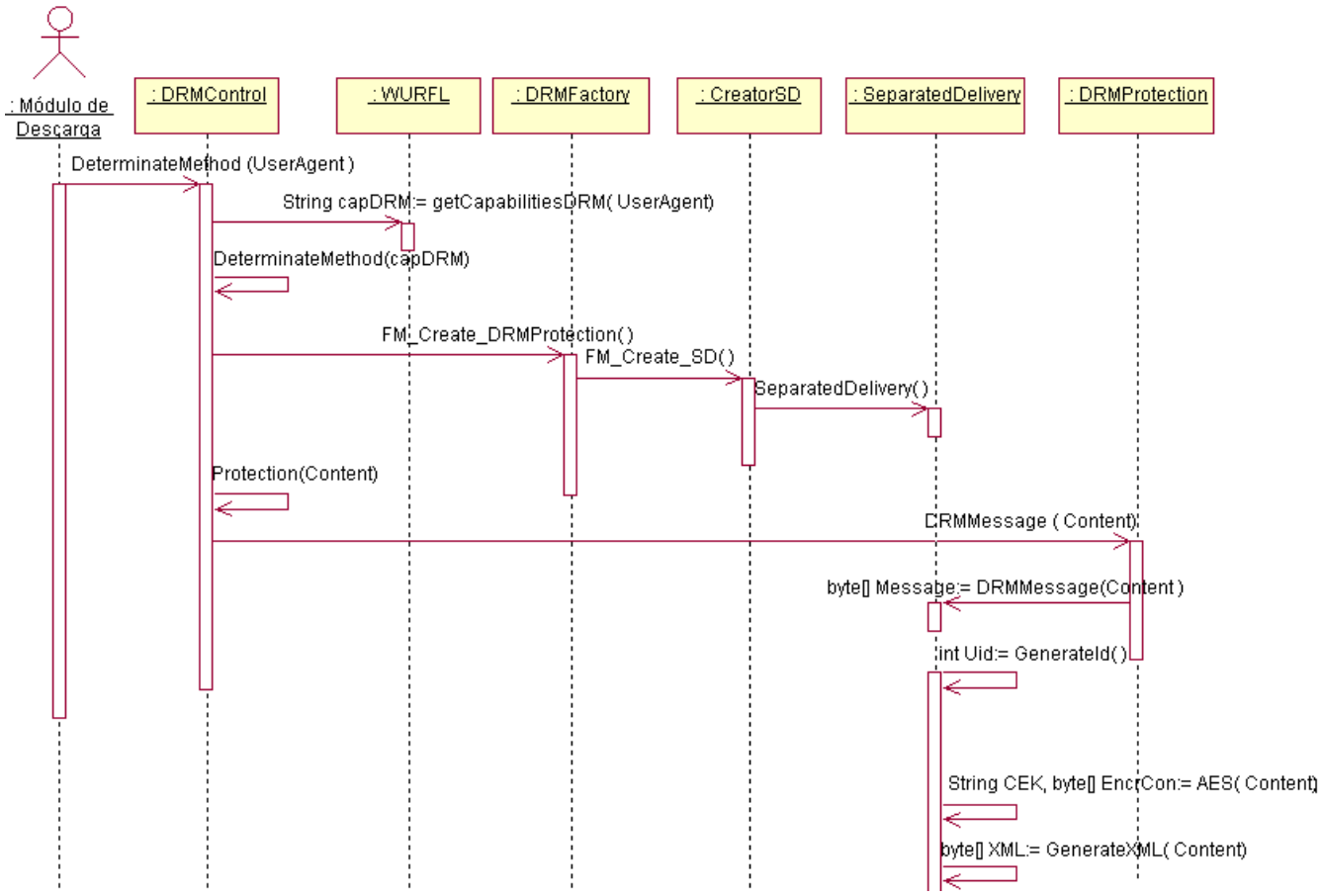

Figura 10a. Diagrama de secuencia CU: Separated Delivery.

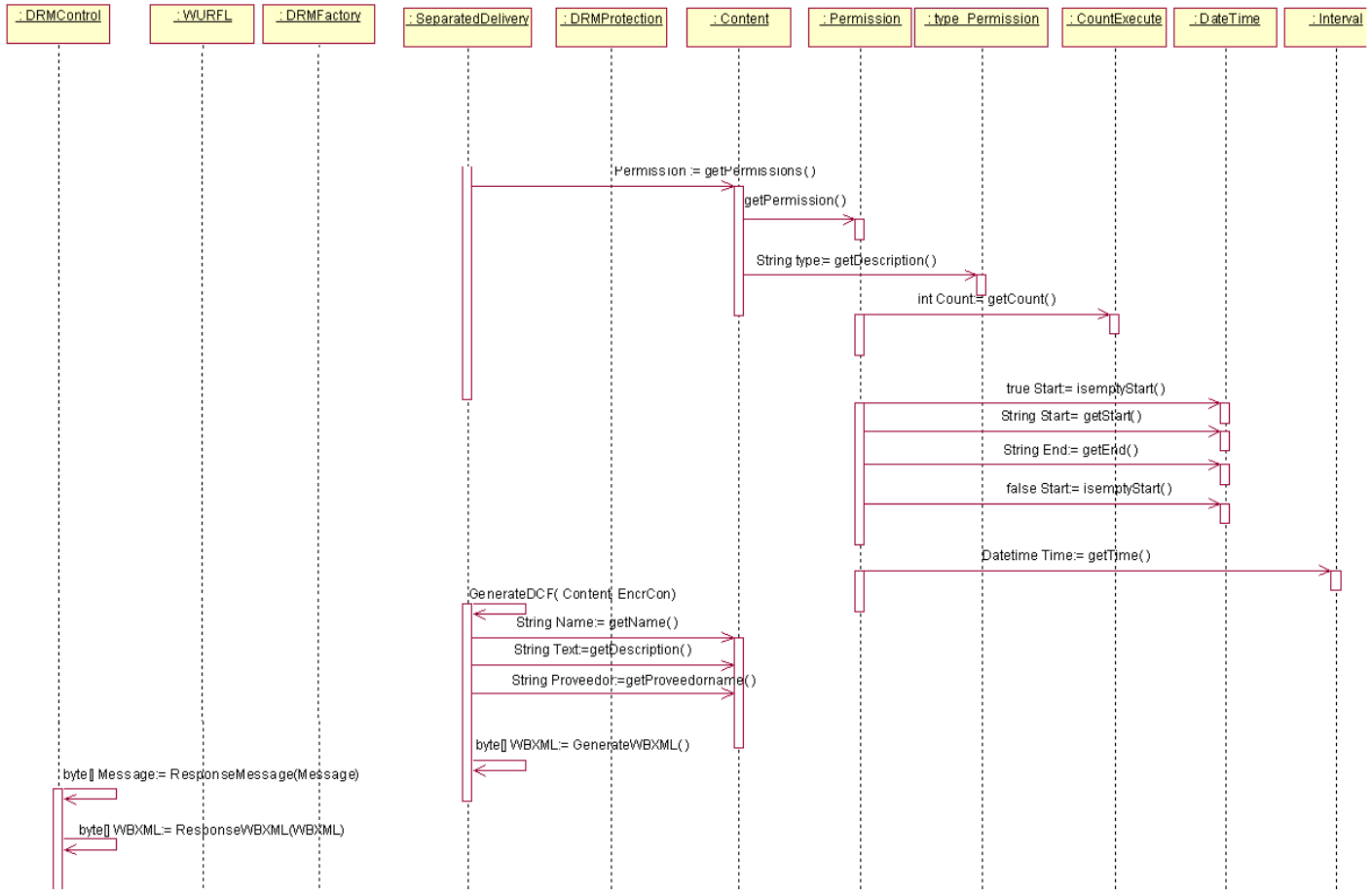

Figura 10b. Diagrama de secuencia CU: Separated Delivery.

Partiendo de que el objetivo fundamental del Moduló de Administración de Derechos Digitales es la protección de contenido y no su gestión, no se identificaron clases persistentes y por consecuente no se diseñará una Base de Datos.

3.10 Conclusiones del capítulo.

En este capítulo se obtuvo el modelo de análisis y diseño de la solución propuesta realizándose los diagramas de clases y de interacción para cada caso de uso del sistema identificado en el flujo de trabajo Requisitos. Se realizó un bosquejo sobre los patrones de diseño aplicados, de forma tal, que este trabajo pueda tener un desarrollo con la calidad requerida y entendimiento para futuros desarrolladores.

Capítulo 4

Estudio de la Factibilidad

4.1 Introducción.

Uno de los principales objetivos del estudio de la factibilidad es disminuir el riesgo que implica todo el proceso investigativo y evitar las pérdidas de recursos que afectan la entidad donde se lleva a cabo el proyecto en caso de que no se obtengan los beneficios esperados. Debido a esto para todo proyecto es de suma importancia el análisis del costo, el esfuerzo y los beneficios que reportará y en este capítulo se describirá esto para el sistema propuesto.

4.2 Planificación basada en Puntos de Casos de Uso.

La especificación de los requerimientos mediante Casos de Uso ha probado ser uno de los métodos más efectivos para capturar la funcionalidad de un sistema. Este hecho se puede apreciar en algunas metodologías actuales ampliamente difundidas, como el proceso Unificado de Rational (Rational Unified Process), en las cuales se propone especificar la funcionalidad de los sistemas mediante la utilización de Casos de Uso.

Se trata de un método de estimación del tiempo de desarrollo de un proyecto mediante la asignación de "pesos" a un cierto número de factores que lo afectan, para finalmente, contabilizar el tiempo total estimado para el proyecto a partir de esos factores.

Paso 1. Factor de Peso de los actores sin ajustar (UAW)

Tabla14 - Factor de peso de los actores sin ajustar.

Tipo de actor	**Descripción**	**Factor de peso**	**Actores**	**Total**
Simple	Sistema con sistema a través de interfaz de programación.	1	1	1

Medio	Sistema con sistema mediante protocolo de interfaz basada en texto.	2	0	0
Complejo	Persona que interactúa con el sistema mediante interfaz gráfica.	3	0	0
	UAW = Σ(Factor * Actores)		UAW	1

Paso 2. Factor de peso de los Casos de Uso sin ajustar (UUCW)

Tabla 15- Factor de peso de los Casos de Uso sin ajustar.

Tipo de CU	Descripción	Peso	Cantidad de CU	Total
Simple	El caso de uso tiene de 1 a 3 transacciones.	5	3	15
Medio	El caso de uso tiene de 4 a 7 transacciones.	10	1	10
Complejo	El caso de uso tiene más de 8 transacciones.	15	0	0
	UUCW = Σ(Factor * CantCU)		UUCW	25

Paso 3. Determinar los puntos de caso de uso sin ajustar (UUCP).

UUCP = UAW + UUCW = 1+ 25 = 26

Paso 4. Determinar los factores de complejidad técnicos (TCF).

El factor de complejidad técnica (TCF) se calcula mediante la cuantificación de un conjunto de factores que determinan la complejidad técnica del sistema. Cada factor se cuantifica en un valor desde 0 (aporte irrelevante) hasta 5 (aporte muy relevante).

Tabla 16- Factor de Complejidad Técnica.

Factor	Descripción	Peso	Valor asignado	Total
T1	Sistema distribuido	2	0	0
T2	Tiempo de respuesta	1	5	5
T3	Eficiencia del usuario final	1	4	4
T4	Funcionamiento Interno complejo	1	5	5

T5	El código debe ser reutilizable	1	4	4
T6	Facilidad de instalación	0.5	3	1.5
T7	Facilidad de uso	0.5	4	2
T8	Portabilidad	2	5	10
T9	Facilidad de cambio	1	4	4
T10	Concurrencia	1	3	3
T11	Incluye objetivos especiales de seguridad	1	5	5
T12	Provee acceso directo a terceras partes	1	0	0
T13	Se requieren facilidades especiales de entrenamiento de usuarios	1	0	0
			Sumatoria	43.5

TCF = 0.6 + 0.01 x Σ (Pesoi x Valor asignadoi)

= 0.6 + 0.01 (Total Factor)

= 0,6 + 0,01 (43.5)

= 0.6 + 0.435

TCF = 1.035 ≈ 1.0

Paso 5. Determinar el factor de ambiente (EF).

El factor de ambiente (EF) está relacionado con las habilidades y entrenamiento del grupo de desarrollo que realiza el sistema. Cada factor se cuantifica con un valor desde 0 (aporte irrelevante) hasta 5 (aporte muy relevante).

Tabla 17- Factor de Ambiente.

Factor	**Descripción**	**Peso**	**Valor asignado**	**Total**
E1	Familiaridad con el modelo de proyecto utilizado	1.5	4	6
E2	Experiencia en la aplicación	0.5	1	0.5
E3	Experiencia en la orientación a objetivos.	1	4	4

E4	Capacidad del analista líder.	0.5	4	2
E5	Motivación.	1	5	5
E6	Estabilidad de requerimientos	2	4	8
E7	Personal Part–Time	-1	0	0
E8	Dificultad del lenguaje de programación	-1	0	0
			Sumatoria	25

EF = 1.4 + (- 0.03 x Σ (Pesoi x Valor asignadoi))

= 1.4 + (- 0.03 x 25)

= 1.4 - 0.75

EF = 0.65

Paso 6. Determinar los puntos de caso de uso ajustados (UCP).

UCP = UUCP x TCF x EF donde,

UCP: Puntos de Casos de Uso ajustados

UUCP: Puntos de Casos de Uso sin ajustar

TCF: Factor de complejidad técnica

EF: Factor de ambiente

(UCP = UUCP x TCF x EF)

UCP = 26 x 1.0 x 0.65

UCP = 16.9

Paso 7. Determinar el esfuerzo.

Para obtener el factor de conversión (CF) se cuentan cuantos valores de los que afectan el factor ambiente (E1...E6) están por debajo de la media (3), y los que están por arriba de la media para los restantes (E7, E8). Si el total es 2 o menos se utiliza el factor de conversión 20 Horas-Hombre / Punto de Casos de Uso. Si el total es 3 o 4 se utiliza el factor de conversión 28 Horas-Hombre / Punto de Casos de uso. Si el total es mayor o igual que 5 se recomienda efectuar cambios en el proyecto ya que se considera que el riesgo de fracaso del mismo es demasiado alto.

En este caso se puede decir que:

CF=20 (Factor de conversión)

E = UCP x CF

E = 16.9 x 20

E = 338 Horas –Hombre

Tabla 18- Esfuerzo del Proyecto.

Actividad	**Porcentaje %**	**Horas-Hombre**
Análisis	10	33.8
Diseño	20	67.6
Implementación	40	135.2
Pruebas	15	50.7
Sobrecarga (otras actividades)	15	50.7
Total	100	338

Esfuerzo ⇒Tiempo

E (total): Esfuerzo Total

CH: Cantidad de Hombres

TDES: Tiempo de Desarrollo

Esfuerzo Total:

TDES (total) = E (total) / CH (total)

TDES (total) = 338 Horas-Hombre / 1 Hombre

TDES (total) = 338 Horas-Hombre

Teniendo en cuenta que en Cuba existen 8 horas laborables al día, trabajando 6 días en la semana, podemos decir que el mes consta de 192 horas laborables.

TDES (total) = 338 Horas/ 192 Horas

TDES (total) = 1.76 Meses-Hombre ≈ 2 Meses-Hombre

Paso 8. Determinar el Costo Total a partir del esfuerzo en HH.

Costo Total (a partir del esfuerzo en HH)

C (total) = E (total MH) x CHM CHH: Costo por Hombre Mes

C (total) = 2 x 100

C (total) = 200 $

Tabla 19- Resultados sobre el estudio de factibilidad.

Valores Finales	
Tiempo de Desarrollo	2 meses
Cantidad de hombres	1 hombre
Costo del desarrollo del sistema	200 $

4.3 Análisis de costos y beneficios.

La integración del Módulo de Administración de Derechos Digitales a la Plataforma de de Gestión de contenido para dispositivos móviles contribuirá a aumentar la calidad de los servicios que se brindan al cliente, la empresa Cubacel, puesto que se le da respuesta a la problemática asociada a la distribución no controlada sobre los contenidos comercializados. Los beneficios hasta el momento son intangibles teniendo en cuenta la adquisición de conocimientos en cuanto a nuevas tecnologías y tendencias del mercado.

La factibilidad del sistema depende del nivel de ventas que tenga. Si la aplicación es comprada, existen varias opciones de pago, una de ellas es que puede ser vendido el sistema completo, si el comprador necesita todas las funcionalidades y el sistema satisface sus necesidades, entonces paga la aplicación y puede además pagar el soporte, si cree que lo necesita.

Teniendo en cuenta el análisis realizado de los beneficios que reporta el diseño del sistema y que no fue necesario realizar inversiones en equipos técnicos para el desarrollo del producto, se concluye que ha sido factible llevar a cabo la realización del software. (14)

4.4 Conclusiones del capítulo.

La factibilidad de un proyecto es un paso muy importante en su desarrollo pues a partir de este punto se decide si se continuará el proyecto o no. En este capítulo se realizó el estudio

de factibilidad mediante el método por Punto de Casos de Uso, el cual permite calcular el tamaño del software, la estimación del esfuerzo y costo del proyecto, concluyendo que el sistema es factible.

Conclusiones

Con el desarrollo de este trabajo, se profundizó en el conocimiento de la tecnología DRM; se aplicó la metodología RUP, para guiar el proceso de desarrollo de software, obteniéndose el diseño del Modulo de Administración de Derechos Digitales con las funcionalidades previstas para la primera versión de la solución y el modelo de diseño se desarrollo aplicando diferentes patrones de diseño el cual es la entrada principal para la futura implementación. Se puede concluir que se ha cumplido satisfactoriamente el objetivo trazado para este trabajo enfatizando en los siguientes puntos:

- Se realizó el estudio detallado del estado del arte de la tecnología DRM
- Se definió la metodología para el desarrollo de la solución.
- Se documentaron las tecnologías y herramientas que se utilizaron para el desarrollo de la solución.

Seguidamente se realizan una serie de recomendaciones que han de tomarse en cuenta para la continuación de la investigación y el desarrollo de los próximos ciclos de desarrollo.

Recomendaciones

A continuación se mencionan algunas recomendaciones con el objetivo de realizar un seguimiento y mejora de esta investigación.

- Para futuras versiones del producto realizar el estudio de otras versiones de OMA.
- Realizar pruebas del módulo con operadores de telefonía móvil.

Bibliografía

1. **Open Mobile Alliance.** OMA. [En línea] [Citado el: 12 de 06 de 2008.] http://www.openmobilealliance.org/Technical/release_program/drm_v1_0.aspx. OMA-Download-DRM-V1_0-20040615-A.

2. **Cátedra Procesamiento de Datos.** Cátedra Procesamiento de Datos. [Online] http://www.ilhn.com/datos/practicos/datosgaby/archives/003121.php.

3. **Organización Mundial de la Propiedad Intelectual.** [Online] http://www.wipo.int/meetings/es/doc_details.jsp?doc_id=29478. Evolución Reciente en el Campo de la Gestión de los Derechos Digitales.

4. **Telefónica.** [Online] [Cited: febrero 4, 2008.] http://www.telefonica.es/sociedaddelainformacion/html/publicaciones_movilidad.shtml. Las Telecomunicaciones yla movilidad en la sociedad de la infroación.

5. **Angel, José de Jesús Angel.** *Advanced Encryption Standard.* 2005. PRINCIPIANTES.

6. [Online] http://biblioteca.uci.cu/sbd/biuci/index.html.

7. Grupo de Traducción al castellano de los RCF. [En línea] http://www.rfc-es.org/descargas.php. RFC2045-es.

8. **Jacobson, Ivar, Booch, Grady and Rumbaugh, James.** *El proceso unificado de desarrollo del software.*

9. **Alexander, Cristopher.** *Patterns.*

10. Introducción a Patrones. [Online] http://www.mcc.unam.mx/~cursos/Algoritmos/javaDC99-2/patrones.html.

11. **Larman, Craig.** *UML y Patrones.*

12. http://www.tripix.net/2006/12/05/wurfl-y-php-programando-web-movil/. [Online]

13. **Rambaugh, James, Jacobson, Ivar and Grady, Booch.** *El lenguaje unificado del modelado. Manual de referencia.*

14. **Mario Peralta.** ESTIMACIÓN DEL ESFUERZO BASADA EN CASOS DE USO. [Online] http://www.itba.edu.ar/capis/webcapis/planma.html.

ANEXOS

Anexo 1 Expansión de Casos de Uso del sistema.

Tabla 20 - Expansión de Protección de contenido.

Protección de contenido.			
Actor	Módulo de Descarga		
Propósito	Identificar el método a utilizar para la protección de contenido.		
Resumen	El caso de uso se inicia cuando el sistema recibe el User Agent que identifica al teléfono que hace la solicitud de descarga, luego accede a las capabilities DRM para analizar los métodos de protección de contenido que soporta el teléfono mediante la información que brinda el User Agent y finaliza determinando qué método utilizar en dependencia de la jerarquía de los mismos.		
Referencias	**RF 1**		
Precondiciones	-		
Requisitos especiales	-		
Curso normal de los eventos			
Acción del autor		**Respuesta del sistema**	
1	Pasa por parámetro el User Agent que identifica el teléfono que realiza la solicitud de descarga.	1.1	Con la información que brinda el User Agent, accede a las capabilities DRM del teléfono para conocer qué métodos DRM soporta para la protección de contenido.
		2	Determina según la jerarquía de los métodos cuál se utilizará para la protección de contenido. Primero verifica si soporta Separated Delivery si es así, entonces se determina este método para

			la protección de contenido.
Curso alternativo de los eventos			
Acción del autor		**Respuesta del sistema**	
		3	De no contener Separated Delivery analiza si soporta el método Combined Delivery, de ser así, se determina este método para la protección de contenido.
		4	Al no presentar los métodos anteriores se aplicará el método Forward Lock para la protección de contenido.
Prioridad	Crítico.		
Poscondiciones	Se identificó el método DRM a utilizar para la protección del contenido.		
Puntos de Extensión	CU Método Forward Lock, CU Método Combined Delivery, CU Método Separated Delivery.		

Tabla 21 - Expansión de Método Forward Lock.

Método Forward Lock	
Actor	Módulo de Descarga.
Propósito	Proteger el contenido que solicitado mediante el uso de algoritmo Forward Lock.
Resumen	El caso de uso comienza cuando el sistema al haber determinado este algoritmo DRM a aplicar, recibe el contenido a proteger para luego armar el mensaje DRM y realizar la solicitud de su entrega.
Referencias	**RF 2, RF5**
Precondiciones	Debe haberse determinado este algoritmo DRM para la protección del contenido.
Requisitos	-

especiales			
Curso normal de los eventos			
Acción del autor		**Respuesta del sistema**	
1	Entrega el contenido a proteger.	1.1	Recibe el contenido y lo convierte en un flujo de bytes.
		2	Arma el mensaje DRM con el contenido convertido, tener en cuenta que el mensaje solo está relacionado con el contenido multimedia, nunca con sus restricciones.
		2.1	Solicita la entrega del mensaje DRM.
Prioridad	Crítico		
Poscondiciones	El contenido está protegido.		

Tabla 22 - Expansión de Método Combined Delivery.

Método Combined Delivery	
Actor	Módulo de Descarga
Propósito	Proteger el contenido mediante el uso del algoritmo Combined Delivery.
Resumen	El caso de uso comienza cuando el sistema al haber determinado este algoritmo DRM, recibe el contenido a proteger generando los Derechos de Uso a partir de las restricciones asociadas al contenido y finaliza obteniéndose el empaquetado del contenido en el mensaje DRM junto a los Derechos de Uso, para luego realizar, la solicitud de su entrega.
Referencias	**RF 3, RF5**
Precondiciones	Debe haberse determinado este algoritmo DRM para la protección del contenido.

Requisitos especiales	-		
Curso normal de los eventos			
Acción del autor		**Respuesta del sistema**	
1	Entrega el contenido a proteger.	1.1	Recibe el contenido del cual analiza las restricciones que tiene asociadas para así generar Derechos de Uso. Primero examina qué acción se puede ejecutar sobre este contenido.
		2	Genera un identificador que describe el momento exacto en que se protege el contenido.
		3	Analiza cuáles son las restricciones que tiene la acción a ejecutar sobre el contenido.
		3.1	Genera los Derechos de Uso en forma de XML, el cual está compuesto por el identificador, la acción que se puede ejecutar sobre el contenido y sus restricciones asociadas.
		4	Convierte el contenido a flujo de datos.
		5	Genera el mensaje DRM teniendo en cuenta que está integrado por dos partes, una para los Derechos de Uso y la otra para el contenido multimedia convertido en flujo de datos.
		6	Realiza la solicitud de entrega del mensaje DRM.
Prioridad	Crítico		
Poscondiciones	El contenido está protegido.		

Tabla 23- Expansión de Separated Delivery.

Método Separated Delivery.			
Actor	Módulo de Descarga		
Propósito	Proteger el contenido que solicitado mediante el uso de Método Separated Delivery.		
Resumen	El caso de uso comienza cuando el sistema al haber determinado este algoritmo DRM, recibe el contenido a proteger encriptando así el contenido y luego armar el mensaje DRM y los Derechos de Uso finaliza obteniéndose al realizar la solicitud de su entrega de los Derechos de Uso y del mensaje DRM por separado.		
Referencias	**RF 4**		
Precondiciones	Debe haberse determinado este algoritmo DRM para la protección del contenido.		
Requisitos especiales	-		
Curso normal de los eventos			
Acción del autor		**Respuesta del sistema**	
1	Entrega el contenido a proteger.	1.1	Recibe el contenido del cual analiza las restricciones que tiene asociadas para así generar Derechos de Uso. Primero examina qué acción se puede ejecutar sobre este contenido.
		2	Genera un identificador que describe el momento exacto en que se protege el contenido
		3	Analiza cuáles son las restricciones que tiene la acción a ejecutar sobre el contenido. Las restricciones son de tiempo, pudiendo estar definidas en un rango donde se especifica el momento en que se comienza y en el que se

			termina; o definido en un valor durante el cual se puede ejecutar esa acción. También existen las restricciones de cantidad de ejecuciones donde se define las veces que se puede ejecutar el contenido.
		4	Encripta el contenido mediante el algoritmo de encriptación simétrico Advanced Encryption Standard (AES) obteniéndose la llave de decodificación Content Encryption Key (CEK).
		5	Crea los Derechos de Uso en forma de XML, el cual está compuesto por : - el identificador, - la CEK, y - la acción que se puede ejecutar sobre el contenido junto a sus restricciones.
		6	Genera el DRM Content Format (DCF) el cual debe contener: - el nombre del contenido, - el identificador generado, - el contenido encriptado, - el nombre del proveedor, y - una breve descripción del contenido.
		7	Comprime el XML de los Derechos de Uso, convirtiéndolos en WBXML.
		8	Genera el mensaje DRM compuesto por el DCF.
		9	Realiza la solicitud de entrega del mensaje DRM y del WBXML de los Derechos de Uso.
Prioridad	Crítico		
Poscondiciones	El contenido está protegido.		

Anexo 2 Formato de los derechos de uso.

Los Derechos de Uso son los permisos y restricciones definidos por el proveedor donde se delimita el acceso al contenido; de los que se genera un XML compuesto por dichas condiciones. A continuación se representan las etiquetas definidas para el XML.

Tabla 24- <rights>

Elemento	<!ELEMENT o-ex:rights (o-ex:context, o-ex:agreement)>
Semántica	El elemento <rights> es el elemento raíz de todas los ficheros que definen las restricciones definidos en la versión 1.0 de OMA. Contiene los elementos <context> y <agreement> los que muestran vínculos a los correspondientes permisos; estos campos son obligatorios.

Tabla 25- <agreement>

Elemento	<!ELEMENT o-ex:agreement (o-ex:asset, o-ex:permission)>
Semántica	El elemento <agreement> especifica los permisos concedidos para sus correspondientes objetivos. Contiene es la raíz de los elementos <asset> y <permission>, estos son obligatorios.

Tabla 26- <asset>

Elemento	<!ELEMENT o-ex:asset (o-ex:context, ds:KeyInfo?)>
Semántica	El elemento <asset> especifica la identidad del contenido gobernado por el elemento <agreement> mediante su elemento hijo <context>. El elemento opcional <KeyInfo> muestra la funcionalidad de acceder al contenido encriptado, en caso de haberse utilizado el algoritmo Separated Delivery. Si el contenido está desencriptado entonces el elemento <KeyInfo> es omitido e ignorado por el agente DRM.

Tabla 27- <context>

Elemento	<!ELEMENT o-ex:context (o-dd:version?, o-dd:uid?)>

Semántica	El elemento < context > contiene los elementos opcionales <version> y <uid>. Como su nombre lo indica, provee información sensible del contenido que es usada dentro el contexto de sus elementos padres. La semántica de sus elementos hijos depende del padre donde se esté usando el elemento <context>. Existe una gran diferencia entre la funcionalidad del elemento <context> cuando es hijo de <right> que cuando es hijo del elemento <asset>. Estas diferencias se detallan en las correspondientes descripciones de los elementos hijos.

Tabla 28- <version>

Elemento	<!ELEMENT o-dd:version (#PCDATA)>
Semántica	El elemento <version> solo debe ser usado si su padre <context> está incluido en el elemento padre <right>. Específica la versión de OMA que se utiliza, en este caso es 1.

Tabla 29- <uid>

Elemento	<!ELEMENT o-dd:uid (#PCDATA)>
Semántica	Su padre es el elemento <context> y es incluido en el elemento <asset>. Especifica el identificador del contenido del contenido DRM. Contiene el valor ContentURI del DCF en caso de que el contenido esté encriptado al usarse el método Separated Delivery; o el encabezado Content-Id que hace referencia al contenido dentro del mensaje DRM en caso del contenido sin encriptar al usarse el método Combined Delivery. El formato usado para este valor debe estar acorde al RFC2396.

Tabla 30- <permission>

Elemento	<!ELEMENT o-ex:permission (o-dd:play?, o-dd:display?, o-dd:execute?, odd:-print?)>
Semántica	Contiene un grupo de permisos opcionales que especifican las restricciones para el contenido, los cuales están definidos en los elementos opcionales

	<play>, <display>, <execute>.

Tabla 31- <play>

Elemento	<!ELEMENT o-dd:play (o-ex:constraint?)>
Semántica	Este elemento concede los permisos de reproducir. Contiene el elemento opcional <contraint>. Si el elemento <contraint> es especificado entonces el Agente DRM debe garantizar la ejecución del permiso de reproducir según describe el elemento hijo <contraint>. Si el elemento <contraint> no es especificado el agente DRM debe garantizar ilimitables ejecuciones para la reproducción del contenido. Soporta contenido de tipo audio/video audio/midi, video/quicktime.

Tabla 32- <display>

Elemento	<!ELEMENT o-dd:display (o-ex:constraint?)>
Semántica	Garantiza la ejecución de los permisos de visualización. Contiene el elemento opcional <contraint>. Si el elemento <contraint> es especificado el agente DRM debe garantizar los permisos de visualización acordes a lo establecido por el elemento hijo <contraint>. Si no es especificado entonces el agente DRM debe garantizar ilimitable ejecuciones para la visualización del contenido. Soporta contenido de tipo image/gif or image/jpeg.

Tabla 33- <execute>

Elemento	<!ELEMENT o-dd:execute (o-ex:constraint?)>
Semántica	Garantiza la cumplimiento de los permisos de ejecución. Contiene el elemento opcional <contraint>. Si el elemento <contraint> es especificado el agente DRM debe garantizar los permisos de ejecución acordes a lo establecido por el elemento hijo <contraint>. Si no es especificado entonces el agente DRM debe garantizar ilimitable ejecuciones para la ejecución del contenido. Soporta contenido como por ejemplo juegos JavaTM u otras aplicaciones.

Tabla 34- <u><contraint></u>

Elemento	<!ELEMENT o-ex:constraint (o-dd:count?, o-dd:datetime?, o-dd:interval?)>
Semántica	Contiene como elementos opcionales <count>, <datatime>, <interval>.

Tabla 35- <u><count></u>

Elemento	<!ELEMENT o-dd:count (#PCDATA)>
Semántica	Especifica el número de tiempo que puede ser concedido un permiso. Posee un valor entero positivo. El agente DRM no puede conceder acceso al contenido DRM más del que se ha especificado en este valor. De manera similar el agente DRM no debe conceder acceso al contenido DRM si este valor es negativo.

Tabla 36- <u><datatime></u>

Elemento	<!ELEMENT o-dd:datetime (o-dd:start?, o-dd:end?)>
Semántica	Especifica el rango de tiempo, respectivamente el tiempo límite para la ejecución de un permiso. Contiene los elementos opcionales <start> y <end>. Si el elemento <start> está presente, semánticamente no debe especificarse delante de time/date. Si el elemento <end > está presente, semánticamente no debe especificarse detrás de time/date Si ambos están presentes, el valor del elemento <start> debe ser más pequeño que el del elemento <end>. Si el valor del elemento <start> es mayor que el del elemento <end> el Agente DRM no debe conceder acceso al contenido DRM acorde a las restricciones establecidas. Si ambas están ausentes el elemento datatime no tendrá significado y será ignorado. El agente DRM de un dispositivo sin una restricción de tiempo no deberá acceder al contenido DRM acorde a los permisos establecidos por el elemento <datatime>.

Tabla 37- <u><start></u>

Elemento	<!ELEMENT o-dd:start (#PCDATA)>
Semántica	Especifica el comienzo de time/ date. Debe cumplir con el formato definido en ISO8601. La representación léxica en formato extendido se representa como CCYY-MM-DDThh:mm:ss donde CC denota el siglo, YY denota el año, MM denota el mes, DD denota el día, T es el separador date/time, y hh, mm, ss representan la hora, minutos, y segundos respectivamente. Por ejemplo, 2002-12-31T23:59:59 representa Diciembre 31, 2002, 23:59:59 hora local. El agente DRM no debe conceder el acceso al contenido DRM antes que no se especifique el valor del elemento <start>.

Tabla 38- <end>

Elemento	<!ELEMENT o-dd:end (#PCDATA)>
Semántica	Especifica el final de time/ date. Debe cumplir con el formato definido en ISO8601. La representación léxica en formato extendido se representa como CCYY-MM-DDThh:mm:ss donde CC denota el siglo, YY denota el año, MM denota el mes, DD denota el día, T es el separador date/time, y hh, mm, ss representan la hora, minutos, y segundos respectivamente. Por ejemplo, 2002-12-31T23:59:59 representa Diciembre 31, 2002, 23:59:59 hora local. El agente DRM no debe conceder el acceso al contenido DRM después que se especifique el valor del elemento <start>.

Tabla 39- <interval>

Elemento	<!ELEMENT o-dd:interval (#PCDATA)>

Semántica	Especifica un periodo de tiempo durante el cual los permisos pueden ser ejecutados sobre el contenido DRM. El periodo <interval> comienza cuando los permisos asociados se ejecutan por primera vez. Los permisos pueden ser ejecutados cualquier número de veces dentro del período <interval>. El agente DRM no debe conceder acceso al contenido DRM después que el período especificado por el valor del elemento <interval> ha transcurrido. El formato general usado para especificar los valores del intervalo son definidos en [ISO8601]. Esta representación léxica es PnYnMnDTnHnMnS, por ejemplo, P2Y10M15DT10H30M20S representa la duración de 2 años, 10 meses, 15 días, 10 horas, 30 minutos y 20 segundos. El agente DRM del dispositivo consumidor sin una restricción de tiempo no debe permitir el acceso al contenido DRM acorde a los permisos descritos en el elemento <interval>.

Tabla 40- <KeyInfo>

Elemento	<!ELEMENT ds:KeyInfo (ds:KeyValue)>
Semántica	Este elemento es el punto de inicio para el control de todo el consumo del contenido, es decir del contenido encriptado. Contiene el elemento <KeyValue>. El elemento se asocia con la correspondiente protección de los objetivos que rigen las restricciones. Este elemento, <KeyInfo>, no debe ser incluido en el elemento <asset> correspondiente al contenido DRM si el contenido no está cifrado.

Tabla 41- <KeyValue>

Elemento	<!ELEMENT ds:KeyValue (#PCDATA)>
Semántica	Este elemento contiene la CEK. Tenga en cuenta que el contenido de este elemento está en formato binario cuando es un WBXML.

A continuación se ilustra con un ejemplo de los Derechos de Uso para el algoritmo Combined Delivery.

<o-ex:rights

> <o-ex:context>

<o-dd:version>1[1]**</o-dd:version>**

</o-ex:context>

<o-ex:agreement>

<o-ex:asset>

<o-ex:context>

<o-dd:uid>cid:4567829547[2]@foo.com[3]**</o-dd:uid>**

</o-ex:context>

<ds:KeyInfo>

<ds:KeyValue> vUEwR8LzEJoeiC+dgT1mgg[4]== /**ds:KeyValue>**

</ds:KeyInfo>

</o-ex:asset>

<o-ex:permission> <o-dd:play/> **</o-ex:permission>**

</o-ex:agreement>

</o-ex:rights>

[1] Versión de OMA DRM, en este caso 1.
[2] Identificador que se genera.
[3] Dominio del servidor donde se publican los Derechos de Uso.
[4] CEK.

Anexo 3 Formato del Mensaje DRM.

Los mensajes DRM son mensajes multipartes (multi-part), en las cuales uno o más conjuntos diferentes de datos están combinados en un cuerpo único.
El cuerpo debe contener pues una o más partes, cada una precedida por una línea con el delimitador, y la última seguida por una línea de cierre de delimitador. Después de su línea de delimitador, cada cuerpo consiste en un área de cabecera, una línea en blanco, y un área de cuerpo. Por tanto una parte de cuerpo es similar a un mensaje RFC 822 en su sintaxis, pero diferente en su significado.
Cada parte del mensaje tendrá como cabecera la palabra reservada Content-Type [RCF 2045] especificando la naturaleza del contenido que sigue a continuación, existe una cabecera global donde el valor del Content-Type dependerá del algoritmo DRM que se utilice, especificando que se trata de un mensaje de una aplicación que responde a la tecnología DRM. En la siguiente tabla se ilustran los posibles mensajes dependiendo del método a utilizar.

Tabla 42- Content-Type para algoritmos de protección de contenido.

Método DRM	**Content-Type**
Forward Lock	application/vnd.oma.drm.*message*
Combined Delivery	application/vnd.oma.drm.*message* y application/vnd.oma.drm.*rights+xml*
Separated Delivery	application/vnd.oma.drm.*rights+xml,* application/vnd.oma.drm.*rights+wbxml* y application/vnd.oma.drm.*content*

Este campo requiere además para entidades multipartes de un parámetro, "boundary", que no es más que la línea del delimitador, se define como una línea que consiste únicamente en dos caracteres guión ("-") seguidos del valor del parámetro "boundary" (delimitador) del campo de

cabecera Content-Type, espacios en blanco opcionales, y un CRLF al final. El “boundary” se declara luego del Content-Type, puede ser cualquier cadena de caracteres, ejemplo “boundary-1”. Se ilustra en el siguiente ejemplo:

Content-type
Boundary= boundary-1
//línea en blanco
—boundary-1
Content-type
Cuerpo 1...
//línea en blanco
—boundary-1
Content-type
Cuerpo 2...
//línea en blanco

El significado del parámetro Content-type depende de la parte del cuerpo donde se utilice. En la parte donde se encuentra el contenido convertido a flujo de byte, este hará referencia al tipo de contenido, su formato general es ***tipo/subtipo***, por ejemplo si es una foto el quedaría de image***/subtipo*** donde el campo subtipo tomará el valor del formato en que se encuentra la imagen (jpg, gif, jpeg, etc).

Cuando el Content-type hace referencia a los Derechos de Uso en el método Combined Delivery su valor sería ***application/vnd.oma.drm.rights+xm***l, ya que su cuerpo corresponde al XML.

En el método Separated Delivery se comprimen el XML de los Derechos de Uso, convirtiéndolos a WBXML, estos son también mensajes DRM, el Content-type tomará como valor ***application/vnd.oma.drm.rights+wbxml.*** Otro proceso que se realiza en este método es la creación de los DCF, donde este campo será ***application/vnd.oma.drm.content***.

Anexo 4 Formato de los DRM Content Format.

La estructura del cuerpo de los DCF debe estar acorde con la siguiente tabla:

Tabla 42- Etiquetas del DCF.

Nombre del campo	Propósito
Version	Número de la versión
ContentTypeLen	Longitud del campo ContentType
ContentURILen	Longitud del campo ContentURI
ContentType	El tipo MIME del cuerpo del mensaje
ContentURI	Un identificador único para el contenido
HeadersLen	Longitud del campo Headers
DataLen	Longitud del campo Data
Headers	Cabecera
Data	Datos encriptados

Version

Este campo define cuál versión del DRM Content Format es usada por el autor. De acuerdo a la versión analizada de OMA DRM el valor del campo debe ser 1.

ContentURI

El ContentURI debe contener un único identificador para el contenido protegido, esto debe ser garantizado por los desarrolladores. Su valor estará acorde a los RFC2392 y RFC2396. Por ejemplo **cid:identificador@dominio**. Como el contenido es referenciado en el XML de las restricciones el valor del campo ContentURI debe coincidir con el valor del campo <o-dd:uid>, ver anexo XML. El dominio es el nombre del servidor donde se publican las restricciones.

Headers

El campo Headers contiene encabezados que definen metadatos acerca del contenido. Estas cabeceras son representadas por nombres similares a las cabeceras HTTP [RFC2616].

Cabecera Encryption-Method

Define cómo el contenido encriptado debe ser desencriptado. Se define de la siguiente forma: Encryption-Method := “Encryption-Method” “:” identificador del algoritmo [“;” parámetro]

identificador del algoritmo:= token.
parámetro:= padding-scheme [";" plaintext-length]

Los valores del identificador del algoritmo se describen como "AES128CBC"

Rights-Issuer

Define la dirección URL donde están publicados de los Derechos de Uso para que el teléfono consumidor pueda acceder.
Rights-Issuer := "Rights-Issuer" ":" url CRLF
url := URI-reference
Este valor debe ser una URL acorde a RFC2396, y debe ser un identificador único.

Content-Name

Contiene del nombre del contenido multimedia protegido. Este nombre es solo informativo.
Content-Name: = "Content-Name" ":" *TEXTO CRLF

Content-Description

Contiene una descripción del contenido multimedia protegido. Este texto también es informativo y puede ser útil para mostrarlo en el dispositivo para mostrarlo antes de obtener los Derechos de Uso en el celular consumidor.

Content-Vendor

Contiene una descripción textual identificando el nombre del proveedor del contenido. Este texto es informativo; puede ser útil para mostrarlo al usuario final antes de obtener los Derechos de Uso.

Anexo 5 Formato de los WBXML.

En el documento Binary XML Content Format Specification se especifican todo lo relacionado al estándar WBXML por ejemplo las conversiones para cadenas de caracteres, números, entre otros; seguidamente se ilustran los tokens relacionados con las etiquetas definidas para el XML.

Nombre del Elemento	**Token WBXML (hexadecimal)**
o-ex:rights	05
o-ex:context	06
o-dd:version	07
o-dd:uid	08
o-ex:agreement	09
o-ex:asset	0A
ds:KeyInfo	0B
ds:KeyValue	0C
o-ex:permission	0D
o-dd:play	0E
o-dd:display	0F
o-dd:execute	10
o-dd:print	11
o-ex:constraint	12
o-dd:count	13
o-dd:datetime	14
o-dd:start	15
o-dd:end	16
o-dd:interval	17

Nombre del Atributo	**Token WBXML (hexadecimal)**
xmlns:o-ex	05
xmlns:o-dd	06
xmlns:ds	07

Valor del Atributo	**Token WBXML (hexadecimal)**	**Comentario**
http://odrl.net/1.1/ODRL-EX	85	Lenguaje de Expresión de Derechos
http://odrl.net/1.1/ODRL-DD	86	Diccionario
http://www.w3.org/2000/09/xmldsig#/	87	XML Digital Signature

Glosario

CRLF: En informática, se refiere a la combinación de dos códigos de control: **CR** (retorno de carro) y **LF** (salto de línea), uno detrás del otro; normalmente con el objetivo de crear una nueva línea.

GPRS: General Packet Radio Service se traduce del inglés como Servicio General de Radio por Paquetes. Es un servicio de datos móvil orientado a paquetes. Está disponible para los usuarios del Sistema Global para Comunicaciones Móviles (Global System for Mobile Communications o GSM).

HTTP: HyperText Transfer Protocol se traduce del inglés como Protocolo de transferencia de Hipertexto. Es el protocolo usado en cada transacción de la Web (WWW). HTTP define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse. HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores.

IVR: Interactive Voice Response, se traduce del inglés como *Respuesta de Voz Interactiva*. Consiste en un sistema telefónico que es capaz de recibir una llamada e interactuar con el humano a través de grabaciones de voz. Es un sistema de respuesta interactiva, orientado a entregar y/o capturar información automatizada a través del teléfono permitiendo el acceso a los servicios de información y operaciones autorizadas, las 24 horas del día.

MMS: Multimedia Messaging System se traduce del inglés como Sistema de Mensajería Multimedia. Es un estándar de mensajería que le permite a los teléfonos móviles enviar y recibir contenidos multimedia, incorporando sonido, video, fotos.

PDA: Personal Digital Assistant se traduce del inglés como Asistente Digital Personal. Es un computador de mano originalmente diseñado como agenda electrónica con un sistema de reconocimiento de escritura. Hoy día se puede usar como una computadora doméstica (ver

películas, crear documentos, juegos, correo electrónico, navegar por Internet, reproducir archivos de audio, etc.).

RFC: Request For Comments se traduce del inglés como Petición de Comentarios. Son una serie de notas sobre Internet que comenzaron a publicarse en 1969.

SMS: Short Message Service se traduce del inglés como Servicio de mensajes cortos. Es un servicio disponible en los teléfonos móviles que permite el envío de mensajes cortos entre teléfonos móviles, teléfonos fijos y otros dispositivos de mano.

TOKEN: Un token de programación, es un elemento individual o un símbolo en un lenguaje de programación.

User Agent: Se traduce del inglés como Agente de Usuario. Es una aplicación informática que funciona como cliente en un protocolo de red; el nombre se aplica generalmente para referirse a aquellas aplicaciones que acceden a la World Wide Web. Los Agentes de Usuario que se conectan a la Web pueden ser navegadores web, pasando por teléfonos móviles, lectores de pantalla y navegadores en braille usados por personas con discapacidades. Cuando un usuario accede a una página web, la aplicación generalmente envía una cadena de texto que identifica al agente de usuario ante el servidor. Este texto forma parte del pedido a través de HTTP, llevando como prefijo User-agent: o User-Agent: y generalmente incluye información como el nombre de la aplicación, la versión, el sistema operativo, y el idioma.

Xerografía: Proceso de impresión que emplea electrostática en seco para la reproducción o copiado de documentos o imágenes. Una superficie es cargada con electricidad estática en forma uniforme. Dicha superficie es expuesta a luz que descarga o destruye la carga eléctrica, quedando cargadas solo aquellas áreas donde hay sombra. Un pigmento de polvo (tinta seca o toner) se fija en estas áreas cargadas haciendo visible la imagen, la que es transferida al papel mediante un campo electrostático. El uso de calor y presión fijan la tinta al papel.

XML: Extensible Markup Language se traduce del inglés como Lenguaje de Marcas Extensible. Es un metalenguaje extensible de etiquetas desarrollado por el World Wide Web Consortium (W3C). No es realmente un lenguaje en particular, sino una manera de definir lenguajes para diferentes necesidades. Tiene un papel muy importante en la actualidad ya

que permite la compatibilidad entre sistemas para compartir la información de una manera segura, fiable y fácil.

WAP: Wireless Application Protocol se traduce del inglés como protocolo de aplicaciones inalámbricas. Es un estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas, por ejemplo acceso a servicios de Internet desde un teléfono móvil. Se trata de la especificación de un entorno de aplicación y de un conjunto de protocolos de comunicaciones para normalizar el modo en que los dispositivos inalámbricos, se pueden utilizar para acceder a correo electrónico, grupo de noticias y otros.

Watermarking: Se traduce del inglés como marca de agua digital. Es una técnica de ocultación de información que forma parte de las conocidas como esteganográficas. Su objetivo principal es poner de manifiesto el uso ilícito de un cierto servicio digital por parte de un usuario no autorizado.