UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

FACULTAD DE INGENIERÍA

PROTECCIÓN DE CONTENIDOS DIGITALES PARA REDES MÓVILES DE TERCERA GENERACIÓN

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

INGENIERA EN TELECOMUNICACIONES

P R E S E N T A :

ORTÍZ ÁNGELES SONIA LIZDE

DIRECTOR DE TESIS: DR. VÍCTOR GARCÍA GARDUÑO

CIUDAD UNIVERSITARIA, D.F. ENERO 2003

A

Agradecimientos.

Quiero darle gracias al amigo incondicional que siempre esta ahí y que sin el nada de esto sería posible a Dios, que me enseño lo siguiente: "No hay amor más grande que dar la vida por sus amigos".

A mis padres Juanita y Mauricio por esa gran tenacidad, ese incorruptible compromiso con la vida y esa enorme creencia en los valores familiares, sociales, religiosos, éticos que cimentaron fuertemente en nosotros.

A mis dos hermanos David y Ariel que siempre han compartido y luchado conmigo por todas aquellas realidades que comenzaron siendo un sueño.

A la Universidad Nacional Autónoma de México por la educación pública y gratuita de excelente calidad que me proporcionó desde el Bachillerato hasta la Universidad.

A la Facultad de Ingeniería, al Departamento de Telecomunicaciones y a sus profesores por forjarme la disciplina del perfeccionismo.

A mi asesor de tesis el Dr. Víctor García Garduño por su optimismo, su entereza y profesionalismo para hacer realidad esta meta.

Al Ing. Carlos Israel León Márquez, por todo su tiempo y apoyo sin medida para la elaboración de este trabajo de Tesis.

A M.I José Ismael por su tiempo dedicado y sus acertados comentarios en el momento adecuado.

A todos áquellos amigos que dejan un fuerte aprendizaje en mi vida: Prof. Luis Alfonso León, Luis Octavio Rámirez, Jessica López, Raúl Juárez, Alfredo Portocarrero, Frida Chávez, Cecilia Vargas, Ángel Arana, Nayeli Chavéz, Ricardo González, Bernardo Pallares, Sergio Rodríguez, Elena Padrino, Vetzcaní Padilla, Ana Lourdes Ortiz, César Carbullanca, Bernarda Ontavaro, Eduardo Torrecilla.

A todos mil gracias Sony.

Índice

INTRODUCCIÓN GENERAL

PAGINACION DISCONTINUA

Introducción General.

A finales del siglo XX, dos inventos revolucionaron la sociedad: la telefonía móvil e Internet. La telefonía móvil permite comunicarnos en movimiento. Internet y sus tecnologías asociadas convierten grandes cantidades de datos en información accesible y servicios de utilidad. Dentro de este cambio, las redes móviles de Tercera Generación integrarán la movilidad con cualquier servicio de Internet.

Las redes móviles actuales fueron diseñadas en un principio para la transmisión de voz y datos utilizando una banda angosta. En este momento, esas redes están evolucionando hacia nuevas tecnologías y métodos que ofrecen mejores velocidades de datos y de acceso para los servicios de Internet Móvil. Al mismo tiempo, se están desarrollando en el mercado recientes aplicaciones totalmente innovadores que requerirán transmisiones de datos de alta velocidad.

La Tercera Generación es reconocida por la convergencia de la voz y los datos con acceso inalámbrico a Internet, utilizando aplicaciones multimedia y con altas tasas de transmisión de datos. Estos sistemas alcanzarán velocidades de hasta 384 Kbps con una movilidad total a los usuarios que viajen a una velocidad de 120 Km /h en ambientes exteriores y alcanzará una velocidad máxima de 2 Mbps con una movilidad limitada a usuarios caminando a menos de 10 Km/h en ambientes estacionarios de corto alcance o en interiores.

La Tercera Generación combina el acceso móvil de alta velocidad con servicios basados en el Protocolo Internet (IP), lo que no solo significa conexiones móviles rápidas a la Web, sino formas completamente nuevas de comunicarse, de acceder a la información, de administrar negocios y de aprender, en contraste con las conexiones antiguas, los equipos voluminosos y lentos y los puntos de acceso inamovibles.

Desde la perspectiva del servicio, la Tercera Generación aportará dos cosas. La primera, los servicios móviles se suministrarán con un mayor rendimiento y una mayor relación costo-eficiencia. La segunda, la Tercera Generación pasará a facilitar nuevos servicios para ampliar los contenidos de información. Por ejemplo, los mensajes móviles de multimedia se tornarán más comunes, lo que constituirá una mejora de los correos electrónicos tradicionales, basados en texto.

El impulso de los estándares de la Tercera Generación culmino en 1999 cuando la Unión Internacional de Telecomunicaciones UIT adoptó un estándar para sistemas inalámbricos de Tercera Generación, conocida como IMT-2000. Con el fin de aprovechar al máximo los beneficios de las inversiones hechas en los sistemas móviles actuales, convino determinar la

manera en que éstos pueden evolucionar hacia la IMT-2000, esto facilitaría la introducción de IMT 2000 y permitirá un mayor grado de reutilización de la infraestructura de las redes existentes. En este sentido la industria global de telecomunicaciones ha reducido en general el número de normas de Tercera Generación, respetando al mismo tiempo las normas existentes. Así se han logrado dos hechos importantes: la convergencia de Time Division Multiple Access (TDMA/136) y Global System for Mobile communications (GSM), y la convergencia de modos Code Division Multiple Access (CDMA).

Como resultado de la evolución y de la convergencia hacia CdmaOne (IS-95A) de banda estrecha existente en los Estados Unidos y en otros países de su área de influencia, se llegó a la tecnología cdma2000 que es una de los cinco interfaces de aire probadas por la UIT para IMT-2000. La norma cdma2000 fue diseñada con una filosofía de independencia de espectro para permitir la migración de los sistemas móviles actuales Personal Communications Service PCS (término genérico para un servicio personal móvil de comunicaciones del mercado masivo, independiente de la tecnología proporcionada) a la Tercera Generación.

En la actualidad el hombre moderno adquiere y experimenta innovadores servicios que posteriormente formarán parte de su vida cotidiana, dentro de los cuales están el e-mail, el comercio electrónico, la música electrónica, el chat, los libros electrónicos, las películas y los juegos, por mencionar algunos. Todos éstos enfocados a una enorme avidez del usuario por la adquisición de información que se convertirá posteriormente en conocimiento y/ o entretenimiento como parte integral de su vida actual.

En el desarrollo de esta tesis, me enfocaré a la problemática del plagio y la piratería de toda información digital que no ha sido protegida y cuyo contenido es extremadamente vulnerable. Dicha problemática surge a consecuencia de una fuerte penetración de Internet en accesos de tipo fijo, donde es conocida la indiscriminada transferencia de información, así como en accesos de tipo inalámbrico con la creación de nuevos servicios agrupados en cinco categorías: a) Acceso a Internet Movil, b) Acceso a las Intranets, c) Infoentretenimiento Personalizado, d) De Multimedia, e) Basados en localización.

Para hacer frente a este problema, varios grupos de la industria musical, editorial, etc. y gigantes tecnológicos se unieron para crear iniciativas para la transformación de sus contenidos a contenidos seguros, e impulsaron fuertemente la Administración de los Derechos Digitales (ADD) en inglés Digital Rights Management (DRM) para la protección de los Contenidos Digitales de los peligros inherentes de su distribución en línea, que en el más básico de lo sentidos, son una propiedad o un trabajo intelectual. En una empresa

cualquier tipo de información o propiedad Intelectual puede ser un contenido; en cualquier caso el contenido es independiente de su formato. Los contenidos pueden ser del tipo: **Texto:** un conjunto de texto y otros activos asociados (como pueden ser imágenes) producidos como libros, documentos, cartas, seguridad de reportes, guías de localización, catálogos, libros de texto, formas, etc. **Audio**: música, llamadas en conferencia, dictados, lecturas. **Video:** películas, conferencias, procedimientos médicos, tours, demos, reuniones, etc. **Imágenes:** fotos, mapas, rayos-x, informes de clima, huellas digitales, etc. **Otros datos:** juegos de multimedia, software, etc.

Los formatos son la envoltura de los contenidos. Por ejemplo, pdf, html, gif, jpg, mp3 ,wav, etc.

La tecnología DRM está surgiendo para la protección y administración de la posesión legítima de la propiedad intelectual y de los derechos de uso de autor.

Esta tecnología está basada en el derecho de copia que se utiliza de forma tradicional, en donde se tiene el siguiente escenario: un libro es adquirido en una librería, una película o documental en una tienda especializada en este tipo de artículos y un disco es comprado en tiendas musicales; lo que implica que físicamente se vaya a los puntos de venta especializados para cada tipo y se adquiriera un artículo, al cual se le asocia un conjunto de derechos de autor que son expedidos por el dueño de la creación (ya sea película, libro o disco), dentro de los cuales se definen reglas o derechos para su empleo categorizados de la siguiente forma: verlo, cambiarlo, imprimirlo, reproducirlo, copiarlo, extraerlo, y/ o traducirlo a otro idioma, asegurando al dueño o publicador que el usuario que adquiera un bien hará un buen empleo de su propiedad. A la evolución tecnológica de estos derechos hacia un mundo digital con contenidos digitales y distribuciones en línea es ahora a lo que le llamamos DRM.

Un sistema DRM está compuesto por entidades que hacen que los contenidos tengan dos características claves que son la fiabilidad y el control, asegurando a los propietarios de dichos contenidos que sus bienes estarán protegidos contra la piratería desenfrenada de millones de cibernautas. Un contenido tratado con los últimos adelantos tecnológicos como algoritmos de encriptación o la manipulación con tecnología watermark o marca de agua hacen al contenido inviolable. Dichas entidades son la generación de licencias, redes de distribución fiables, mecanismos para el cobro de regalías por la obtención y uso de los contenidos, y por último, un software afín a DRM que haya sido desarrollado o que sea capaz de reproducir este contenido protegido

El objetivo de esta tesis es:

- Realizar una investigación que esta sustentada en documentación existente acerca del Sistema DRM. Con base en esto se generó una recopilación de información de los siguientes temas, los cuales también conforman la organización del presente trabajo por capítulos
    - La evolución de los servicios y aplicaciones en redes móviles hacia la Tercera Generación con el objetivo de realizar una descripción de los servicios y aplicaciones que surgirán en dicha Generación.
    - El panorama de la Protección de la Propiedad Intelectual de los Contenidos Digitales como la base en la cuál se estructura un Sistema DRM
    - DRM (Digital Rights Management), como un sistema que provee una solución para evitar el uso indebido de contenidos digitales.
    - Las Herramientas Utilizadas para la Protección de los Contenidos Digitales en las cuales se considera como punto crítico los algoritmos utilizados en el cifrado y el embebido de marcas de agua en los contenidos digitales.
    - La solución DRM-Lite para la protección de contenidos digitales en función tanto del peso del contenido, su costo de creación y de su distribución.
    - Estandarización y Soluciones de Proveedores para la Protección de Contenidos Digitales y la implementación de soluciones propietarias que hoy día se están vendiendo en el mercado digital.

Con el fin de presentar un estudio el cual englobara la evolución, la adaptación, los actores involucrados y el estado del arte de esta nueva tecnología Digital Rights Management (DRM), para solucionar el problema actual que se presenta cuando los usuario deliberadamente obtienen, copian, reproducen y transmiten contenidos digitales que no están protegidos, ocasionando así grandes pérdidas financieras a los diferentes integrantes en la cadena de valor de los contenidos.

Capítulo 1

Evolución de los servicios y aplicaciones en la telefonía celular hacia la Tercera Generación.

1 Evolución de los servicios y aplicaciones en la telefonía celular hacia la Tercera Generación.

1.1. Introducción.

La telefonía móvil nos permite comunicarnos en movimiento. Internet y sus tecnologías asociadas convierten grandes cantidades de datos en información accesible y servicios de utilidad.

En su incorporación al poder de la movilidad, los usuarios esperan servicios de usuario final allí donde se encuentren, e independientemente del tipo de acceso o variedad del dispositivo o terminal. Para conseguirlo, los operadores habrán de disponer de una infraestructura que soporte servicios a través de redes diferentes y separadas; necesitarán una infraestructura de red multiservicio que integre transmisiones de voz, IP, datos y multimedia.

Las principales capas de la nueva arquitectura de comunicación son:

- **La capa de aplicaciones para el usuario**, que define los servicios que crearán ingresos basados en acceso y cantidad de datos. Los Socios, los proveedores independientes de software y las distintas partes de la industria desarrollarán y comercializarán aplicaciones específicas para los usuarios.
- **La capa de aplicaciones de comunicación y control**, esta capa formará parte de un lote de servidores con diferentes capacidades de servicio. Se está estudiando la vía para permitir que los operadores empleen una solución centralizada de Administración para toda su red, de forma que la Administración de la red y de conflictos empleen un sistema único integrado de modo transparente adonde esté situado.
- **La capa de acceso /transporte /troncal**, que es una "gran tubería de bits", es un mecanismo de transporte independiente del medio (voz, datos o multimedia). Esta capa puede y será construida con equipamiento IP y Asynchronus Transfer Mode (ATM) sobre radio, y redes de cable y fibra.

1.2. Escenarios del futuro, retos y perspectivas

La creciente penetración de los sistemas móviles propiciada por el atractivo de mayores velocidades y mejores valores añadidos de la Tercera Generación, permitirá que los ingresos por servicios crezcan espectacularmente.

Un reciente estudio dirigido por el Universal Mobile Telecomunications System UMTS Forum (Informe No. 9 del UMTS Forum): "The UMTS Third Generation Market – Structuring the Services & Revenues Opportunities") sobre las oportunidades de ingresos por servicios, predice una tasa de crecimiento anual que superan los 350.000 millones de dólares en 2010. Esta estimación parcial es impresionante si se compara con las cifras actuales a nivel mundial para todos los servicios móviles celulares: alrededor de 160.000 millones de dólares. En otras palabras, los ingresos resultantes de las nuevas aplicaciones móviles multimedia que posibilitará la Tercera Generación ascenderán a más de la mitad de los ingresos brutos actuales de todo el tráfico móvil.

Uno de los requisitos previos para adaptar con éxito los servicios móviles de Tercera Generación es un marco regulatorio prudente que permita a los operadores construir redes con costos adecuados, al tiempo que facilite a los abonados disfrutar con la máxima utilidad todas las ventajas de la Tercera Generación a un precio justo y equitativo.

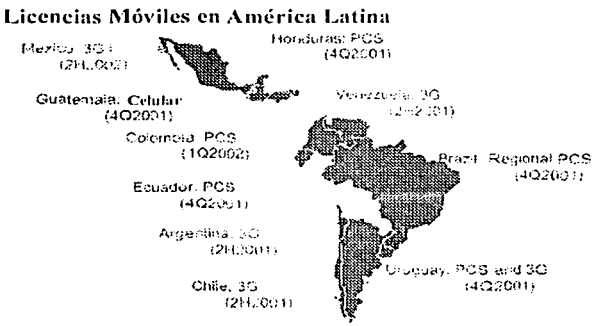
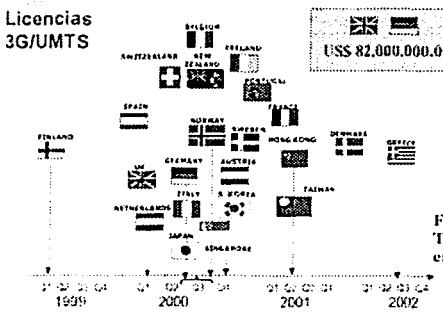


Figura 1.1 Fechas propuestas para Licencias de Tercera Generación en América Latina.



El proceso de concesión de licencias para la Tercera Generación, ya sea por **concurso o subasta**, está ahora en pleno apogeo. Algunas de estas subastas han generado ingresos tan elevados que la industria ha expresado su preocupación sobre el impacto que podrán tener estas tasas sobre las tarifas de usuario y el crecimiento de los servicios de la Tercera Generación. Algunas Administraciones que utilizan el sistema de concurso para seleccionar a los licenciatarios se han animado también a pedir tasas de licencias muy altas.

Figura 1.2. Fechas de adopción de Licencias de Tercera Generación/ UMTS en países con alta penetración de telefonía móvil.

1.2.1. Nuevo enfoque

El punto de convergencia para el suministro de información y entretenimiento –el Portal Multimedia Móvil– será el punto de entrada preferido del usuario para todos los servicios y contenidos basados en IP. El portal ofrece una enorme oportunidad de mercado para construir las fuertes relaciones con el cliente que son esenciales para triunfar competitivamente en el nuevo entorno proporcionado por Internet.

Mientras que los portales fijos tradicionales se diseñan para organizar la entrega de información a segmentos específicos del mercado, el portal móvil estará orientado hacia usuarios individuales y satisfacerá sus necesidades por un acceso robusto y seguro en circunstancias y localizaciones cambiantes. Utilizando una plataforma inteligente de acceso a IP con capacidades de selección dinámica de servicios, el propietario del portal podrá proporcionar servicios personalizados dependientes de la localización, que se ajusten a la medida de las necesidades y de las elecciones individuales de los usuarios móviles.

El acceso inalámbrico a Internet impulsará el desarrollo de la Tercera Generación por varias razones:

- Las tecnologías inalámbricas permiten a los prestadores de servicio y a los negocios en Internet aumentar la cultura móvil y el consumo de servicios.
- La movilidad y la inmediatez ofrecidas por las tecnologías inalámbricas permiten a los distribuidores de contenidos de Internet y al comercio electrónico no estar vinculados a una localización.

- La naturaleza personal de los servicios móviles permiten a las compañías desarrollar perfiles de clientes que facilitan la distribución de información de valor agregado de forma más focalizada.
- Las facilidades y servicios basados en localización proveen otro nivel de conocimiento del cliente que permite a los negocios de Internet distribuir servicios específicamente adecuados.

1.3. Servicios y aplicaciones basados en Tercera Generación

1.3.1. Los nuevos servicios

Las nuevas oportunidades de negocio que introduce Tercera Generación están añadiendo nuevos segmentos de mercado en las telecomunicaciones existentes y tradicionales. Tercera Generación ofrecerá nuevas posibilidades para la provisión de servicios, muchos de estos, si bien empezarán a prestarse en 2G, resultarán más asequibles económicamente en Tercera Generación. Otros servicios ya existentes experimentarán considerables mejoras gracias a las nuevas funcionalidades de localización, interactividad y multimedia móvil, con segmentación de clientes basada en el estudio de los distintos estilos de vida. La demanda de mayor productividad personal será también importante. Y continuarán difuminándose las fronteras entre los mercados de negocios y del gran público, así como entre la oficina y el hogar.

1.3.2. Categorías de servicios

Hasta ahora, la simple clasificación de servicios entre voz y datos era suficiente. La definición del universo de servicios era casi trivial. En el mundo de la Tercera Generación, definir un único conjunto de categorías de servicios es una tarea muy difícil. Estas dificultades reflejan la riqueza de oportunidad abierta para la Tercera Generación. Comencemos identificando seis posibles categorías de servicios que en principio reúnen a la mayoría de la demanda de servicios Tercera Generación de los próximos 5 años. La definición de estas seis categorías de servicios está determinada desde la perspectiva del usuario e intentan reflejar la percepción que tiene el mercado. Existe una lógica evidente detrás de estas seis categorías de servicios como se pone de manifiesto en el siguiente diagrama.

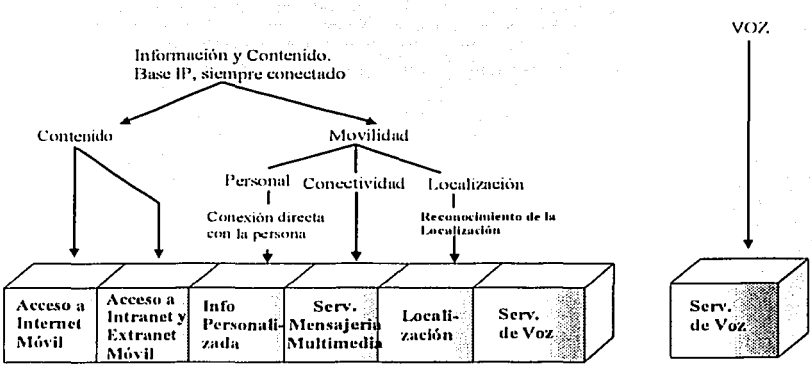


Figura 1.3 Clasificación de Servicios de Tercera Generación.

A diferencia del ambiente centrado en la voz que ha primado hasta hoy en el mundo móvil, Tercera Generación será un ambiente de datos, siempre conectado. La posibilidad de ofrecer conectividad a contenidos de Internet todo el tiempo y "en todo lugar" será un rol fundamental de los sistemas Tercera Generación. Los usuarios estarán en condiciones de agregar movilidad a su experiencia en Internet fija.

Pero la movilidad no es el único beneficio a proveer por estas redes. Las redes móviles proveen dos características diferenciales que la distinguen de las redes fijas. El terminal móvil esta asociado a una persona más que a un lugar y la red conoce la localización de esa terminal. La asociación de una terminal con una persona permitirá la provisión de un conjunto muy grande de servicios de contenidos basados en Internet que se adecuan especialmente a las necesidades del usuario.

El conocer la actual posición de una terminal móvil (la cual puede ser asociada a una persona o a una máquina) está generando un portafolio muy rico de Servicios Basados en la Localización. Nuevamente aquí, la combinación de una conexión permanente con capacidades multimedia disponibles en Tercera Generación suma una nueva dimensión a esta categoría de servicios. La tecnología de localización no solo permite Servicios Basados en Localización sino también mejora la oferta de servicios tales como Infoentretenimiento Personalizados y dará mucho impulso para la creación de nuevas aplicaciones.

La Voz seguirá siendo un servicio muy importante en el ambiente de la Tercera Generación. A estos servicios de Voz se le agregará la capacidad de videoteléfono haciendo uso de las altas velocidades de transmisión de datos. El ambiente IP permitirá a la Tercera Generación proveer comunicaciones multimedia a los servicios de voz.

En resumen, el siguiente cuadro presenta las principales características de estas seis categorías de servicios.

Servicio	Descripción
Acceso a Internet Móvil	Un servicio Tercera Generación que ofrece acceso móvil a todos los servicios provistos por ISP con calidad y funcionalidad casi iguales a las provistas por las redes cableadas Incluye navegación de la Web, transferencia de archivos y visualización de video en tiempo real, con la recepción de pequeños paquetes de video y audio
Acceso Internet/Extranet Móvil	Un servicio corporativo Tercera Generación que provee acceso móvil seguro a Redes de Área Local (LAN) y Redes Privadas Virtuales (VPN) corporativas
Infoentretenimiento Personalizado	Un servicio Tercera Generación para consumidores que provee acceso independiente del terminal de usuario para la personalización de contenidos en cualquier momento y "lugar"
Servicio de Mensajería Multimedia	Un servicio Tercera Generación a consumidores, que ofrece mensajería multimedia en tiempo real con capacidades de conexión permanente para proveer mensajes en forma instantánea. Se podrán establecer grupos definidos por el proveedor del servicio o por los usuarios
Servicios Basados en Localización	Un servicio a corporaciones y consumidores que permite localizar personas, vehículos o máquinas También permite a terceros ubicar al usuario, así como también, permite a los usuarios identificar su propia ubicación a través de la identificación del terminal o vehículo
Voz (incluye comunicaciones de video y multimedia)	Un servicio Tercera Generación bidireccional y en tiempo real. Provee capacidades avanzadas de voz (tales como voz sobre IP, acceso a redes, activado por voz, llamadas vocales mejoradas en la Web) mientras continúa ofreciendo servicios móviles de voz tradicionales. A medida que este servicio madure, irá incluyendo videotelefonía y comunicaciones multimedia móviles

Son los servicios que surgen de la convergencia de la computación, la informática y los medios de comunicación masiva. La exposición a servicios y aplicaciones multimedia en las actuales redes fijas, combinada con el incremento de demanda de movilidad creará expectativas para la provisión de estos servicios para usuarios en "cualquier lugar en que se encuentren". Por ello, es evidente que los servicios fijos multimedia actuarán como precursores de aquellos servicios multimedia móviles.

Podemos identificar cinco categorías genéricas de servicios: servicios audiovisuales pasivos (TV de paga, video bajo demanda, TV corporativa, servicios de audio pasivo, audio bajo demanda), servicios de información, educación y entretenimiento (educación, entretenimiento y juegos; información pública, información turística , compras y trámites bancarios domiciliarios; diarios, revistas; cotizaciones), servicios de comunicaciones personales (videotelefonía, telemedicina, videoconferencia) y servicios corporativos de comunicaciones (interconexión LAN-LAN y acceso a Intranet).

Adicionalmente a los servicios de comunicaciones personales, los sistemas de Tercera Generación podrán proveer una amplia gama de servicios de comunicación máquina a máquina. También se da una gran importancia a la habilidad de ofrecer los mismos servicios que el usuario tiene en su red original cuando se encuentre itinerando en otras redes. La portabilidad de servicios será una capacidad muy importante a ser soportada por las redes de Tercera Generación.

Es importante insistir aquí que el gran potencial de Tercera Generación deriva de las características únicas de su ambiente multimedia móvil más que por sólo agregar movilidad a Internet. La asociación de una dirección de una terminal de usuario con una persona, más que con un lugar, abre la enorme posibilidad a lo que damos en llamar Servicios Multimedia Personalizados a través de los Servicios de Infoentretenimiento Personalizados y de Mensajería Multimedia. Finalmente, el conocimiento de la posición de la terminal, permite el desarrollo de una rica gama de Servicios Basados en Localización.

1.4. Nuevos modelos de negocio

Para sobrevivir, los nuevos entrantes a la Tercera Generación, se deben adoptar nuevos modelos de negocio que conduzcan a la creación de mercados nichos de contenidos, infraestructuras y venta de servicios. Estos mercados nichos podrán sostenerse mediante acuerdos comerciales, estableciendo mecanismos de creación de valores recíprocos, siendo el usuario el gran beneficiario.

1.4.1. Servicios de datos (Contenidos Digitales).

Los operadores móviles ven los servicios de datos como decisivos para aumentar los ingresos medios por usuario y como un factor diferenciador en reserva para cuando los servicios de voz se conviertan en artículos de consumo habitual.

El establecimiento de alianzas y asociaciones serán un factor clave de éxito, particularmente en los servicios vinculados a contenidos móviles. Las alianzas entre proveedores de

contenidos y prestadores de servicios que capitalicen sus respectivas fortalezas son claves para el éxito, estén estas alianzas organizadas bajo la forma de sociedades compartidas o a través de mecanismos tales como prestadores virtuales de servicios móviles.

Una dimensión vital para el éxito de Tercera Generación es la habilidad itinerante para todas las capacidades de servicios en un escenario internacional o interregional. Sin estas capacidades, los datos móviles se verán restringidos a un simple servicio de accesos inalámbrico. La necesidad de servicios itinerantes en ambientes móviles genera una gran demanda en la portabilidad de servicios y reclama soluciones aún no resueltas en temas vinculados a facturación y tarificación entre prestadores de servicios.

Son claras la ventajas significativas que podrán obtener aquellos prestadores de servicios que puedan construir una presencia regional (ya sea a través de ser propietarios o por medio de alianzas) y puedan integrar procedimientos de negocios y ofertas comerciales para proveer servicios a clientes a través de las fronteras nacionales o regionales. En el mundo de la Tercera Generación no todos los suscriptores móviles comprarán todos los servicios Tercera Generación ni todos los suscriptores comprarán la misma cantidad o mezcla de servicios.

El ingreso por contenidos, aun en el caso que este provenga de publicidad, constituirá una porción significativa del total de ingresos cobrados por servicio, en adición a los ingresos del operador de la red o prestador de servicio generados por la distribución del servicio.

Esto demuestra que terceras partes proveedoras de información y programación se beneficiarán con el mercado masivo de servicios móviles multimedia y de esta manera beneficiarse de la minimización de los costos de los servicios a los usuarios finales para hacer frente el desarrollo de este mercado.

La facturación estará basada en disponibilidad, tipo de datos o volumen. La clave de una facturación eficaz será la flexibilidad.

Además, existe la oportunidad de convertirse en un agente mayorista para los proveedores de contenido. No existirá un modelo de negocio, sino una serie de modelos diferentes. A medida que la cadena de valor evoluciona y se vuelve más compleja, se espera que aparezcan muchos de los nuevos actores, tales como agentes de información, integradores de información y desarrolladores de aplicaciones.

1.5. Normalización de los sistemas móviles

Hoy, las numerosas compañías que han hecho de la normalización un elemento técnico y comercial esencial de sus actividades saben que, si ellas no participan, corren el riesgo de

tener que sufrir unas normas que difícilmente tomarán en cuenta sus intereses. El estado actual de la normalización de los sistemas móviles de Tercera Generación es el resultado de los trabajos llevados a cabo en numerosos países desde 1986, fecha en la que comenzaron las tareas de normalización del Future Public Land Mobile Telecommunication System (FPLMTS) iniciadas por la Unión Internacional de Telecomunicaciones - Radio (UIT-R), Grupo de Estudio 8.

En Europa, el programa RACE I, lanzado en 1988, comenzó el trabajo básico de investigación. Este fue seguido por el programa RACE II durante los años 1992-95 que condujo al desarrollo de los prototipos del CDMA y del Advanced Time División Multiple Access (ATDMA).

La normalización Europea de la radio Tercera Generación alcanzó su "fase más caliente" durante 1997, cuando cinco sistemas candidatos fueron considerados por el comité SMG (Grupo Especial de Móviles) del European Telecommunications Standards Institute (ETSI). Después de un largo debate, en enero de 1998 el ETSI SMG acordó usar finalmente la tecnología Wideband CDMA (WCDMA) para la interfaz aire del Universal Mobile Telecommunications System Terrestrial Radio Access (UMTS UTRA) sobre bandas de frecuencias apareadas para el funcionamiento de las tecnologías Frequency Division Duplex (FDD) y Time Division CDMA (TDCDMA) y asignaciones del espectro no emparejadas para el funcionamiento del Time Division Duplex (TDD). Esta decisión fue la base para la propuesta del UTRA presentada por el ETSI a la UIT como una candidata a la tecnología de transmisión radio IMT2000.

Al mismo tiempo, otros países como Japón, Estados Unidos y Corea, fueron eligiendo independientemente sus propias tecnologías de acceso radio Tercera Generación, con Corea, Japón, Europa y uno de los comités norteamericanos (T1P1) seleccionando soluciones similares. Se hizo evidente que sería muy difícil alcanzar especificaciones idénticas para asegurar una compatibilidad global de los equipos – que era un requisito crucial – con todo este trabajo realizándose en paralelo.

Sin embargo, hubo iniciativas para crear un foro único para la normalización de una especificación común del UTRA. El proyecto Tercera GeneraciónPP (3rd Generation Partnership Project) fue establecido en 1998 con este objetivo en mente. En él participan los siguientes socios: TTC/ARIB por Japón, ETSI por Europa, TTA por Corea, T1P1 por EE UU. y, más recientemente (1999), CWTS por China.

Casi al mismo tiempo, el mercado celular norteamericano creó el grupo Tercera GeneraciónPP2 para trabajar sobre la tecnología de radio rival cdma2000, y el Universal Wireless Communication Consortium (UWCC) fue ampliado para cubrir la tecnología UWC136 ó IMT-SC (Single Carrier). Estos dos grupos industriales se apoyan en los 41 protocolos de movilidad del American National Standards Institute (ANSI) definidos en el comité TIA TR45.2.

Los dos consorcios, junto con el UWCC y el proyecto ETSI que trabajan sobre el sistema Digital Enhanced Cordless Telecommunication de 2 Mbit/s (DECT), están trabajando a través de sus propios organismos de normalización para completar el marco UIT para las tecnologías radio para el IMT2000.

Unión Internacional de telecomunicaciones (UIT)

La UIT tiene varios grupos trabajando en el IMT2000 (el término genérico oficial para los móviles Tercera Generación). Dentro del UIT-T, el principal grupo es el nuevo Special Study Group (SSG) IMT2000, mientras que el liderazgo en UIT-R está ahora asignado al Working Party WP8F, que sustituye a los antiguos grupos TG8/1 y WP8/13.

Universal Wireless Communications Consortium UWCC

La Universal Wireless Communications Consortium (UWCC) es una asociación internacional fundada en 1996, de más de 100 operadores y vendedores que apoyan las normas tecnológicas TDMA, Enhanced Date rates for Global Evolution (EDGE), UMTS y Wireless Intelligent Network (WIN). El propósito de esta organización sin propósito de lucro y cooperativa es el de promover TDMA, EDGE, UMTS, y WIN como tecnologías inalambricas de comunicacion globalmente integrada, ofreciendo a los operadores y abonados servicios flexibles y compatibles que están evolucionando en servicios adicionales y que tienen un mejor desempeño de voz y datos

Internet Engineering Task Force (IETF)

El Internet Engineering Task Force (IETF) está cada vez más involucrado en los aspectos de las normas móviles conforme se introduce la tecnología IP en las redes móviles. Los grupos de trabajo principales para la movilidad de la Tercera Generación son MOBILEIP (para la movilidad), SIP (para el control de las llamadas basado en IP) y SIGTRAN (para la transmisión de señalización).

Tercera GeneraciónPP2

En Estados Unidos, de manera similar, la TIA ha puesto en marcha Tercera GeneraciónPP2, con el objetivo de estandarizar la tecnología de acceso radio cdma2000, así como las interfaces hacia las redes centrales ANSI-41.

UMTS FORUM

En la implantación de los sistemas Tercera Generación juega un papel importantísimo el Foro UMTS, un organismo independiente creado en diciembre de 1996 en el que participan casi 170 compañías de 30 países pertenecientes a las industrias suministradoras de equipos, operadores de telecomunicaciones y organismos de regulación. El Foro está comprometido en la formación del consenso necesario para introducir y desarrollar con éxito el estándar UMTS y así poder satisfacer la demanda del mercado de comunicaciones móviles personales de bajo costo y alta calidad.

El Foro UMTS también actúa como catalizador con las organizaciones especializadas que tratan sobre la estandarización y el espectro y entre otros aspectos mantiene relaciones con organizaciones de carácter regional y mundial, con organismos de estandarización y con otras comunidades reconocidas tanto de la industria como de los operadores.

1.6. Evolución de CDMA a cdma2000.

1.6.1. Evolución Histórica de CDMA

En Nov 89 - Primera demostración (San Diego, California), 1993 - Configurado el estándar IS-95ª, Sep 95 - Primer lanzamiento comercial de cdmaOne (Hutchison Telecom, en Hong Kong), Dic 95 - Aparece el decodificador de voz a 13 Kbps, implementado por el CDG, Mar 96 - Primer lanzamiento en Estados Unidos de cdmaOne (BAM), Oct 96 - Primer sistema PCS basado en CDMA en EEUU (PrimeCo Personal Communications), Dic 96 - Primer lanzamiento de cdmaOne en América Latina (Telefónica del Perú), Abr 97 -Primer lanzamiento de cdmaOne en Canadá (TELUS Mobility, antiguamente BCTEL Mobility), May 97 - Primer lanzamiento de un sistema WLL basado en CDMA (MTNL, India), Jun 97 - La marca cdmaOne designa a la especificación IS-95 CDMA, Jun 97 - Es completado el estándar IS-95B, el cual incluye datos a 64 Kbps, Sep 97 - cdmaOne alcanza 4,250,000 suscriptores en todo el mundo, Oct 97 - Primer lanzamiento en Canadá de un sistema PCS basado en CDMA (Bell Mobility and Clearnet Communications), Dic 97 - cdmaOne alcanza 7,800,000 suscriptores en todo el mundo, Mar 98 - cdmaOne alcanza 9,225,000 suscriptores en todo el mundo, Mar 98 - LG Telecom lanza el primer servicio de datos CDMA, Abr 98 -

Se definen los requerimientos para cdma2000, (llamado también 1XRTT). **Abr 98,** la Asociación de la Industria de la Información (TIA, EEUU) endosa cdma2000, como una solución de tercera generación en la UIT. **May 98** - Las dos más grandes ciudades de Brasil, Sao Paulo y Rio de Janeiro, adoptan cdmaOne, **Jun 98** - Venezuela: Telcel y Lucent pactan red CDMA, Jun 98 - Sometido cdma2000, submitted a la ITU para IMT-2000, **Jun 98** - cdmaOne alcanza los 12,130,000 suscriptores en todo el mundo. **Sep 98** - cdmaOne alcanza los 16, 000, 000 suscriptores en todo el mundo. **Oct 98** - Los operadores comienzan discusiones sobre la armonización de las propuestas CDMA IMT-2000. **Dic 98** - cdmaOne alcanza los 23,000,000 suscriptores en todo el mundo. **Feb 99** -Venezuela: Lucent completa actualización de red CDMA de Telcel, **Mar 99** - cdmaOne alcanza los 28,515,000 suscriptores en todo el mundo. **Abr 99** - Japón completa el despliegue de una red nacional cdmaOne. Unas 814,200 personas se afilian al sistema. **May 99** - Los operadores completan el acuerdo de armonización para IMT-2000. **Jun 99** - cdmaOne alcanza los 33, 621,544 suscriptores en todo el mundo. **Jun 99** - China Unicom se afilia al CDG y anuncia planes para ofrecer servicios comerciales. **Jul 99** - Es completada la fase uno del estándar cdma2000. Se aprueba su publicación. **2 Trimestre 99** - Operadores de EEUU, Corea y Japón comienzan a ofrecer servicios de información e Internet basados en cdmaOne. **Ago 99** - La operadora Telstra inicia servicios comerciales, convirtiéndose Australia en el vigésimo noveno país en seis continentes con cdmaOne. **Sep 99** - cdmaOne alcanza 41,140,130 suscriptores en todo el mundo. **Nov 99** - El Grupo de Estudios 8 de la UIT-R coloca los estándares IMT-2000 en fase de votación. **Nov 99** - El Grupo de Tareas 8/1 de ITU-R endosa los estándares CDMA (en sus tres modalidades) para IMT-2000. **Dic 99** - cdmaOne alcanza los 50.1 millones de suscriptores en todo el mundo. **Ene 00** - PacketOne, el servicio de transmisión de paquetes para teléfonos celulares con una velocidad máxima de 64 Kbps, es lanzado en todo EEUU. **Feb 00** - Motorola and Sprint PCS logran interoperabilidad comercial inalámbrica. **Mar 00** - La mexicana Iusacell se convierte en la primera operadora latinoamericana en ofrecer servicios inalámbricos Internet. **Abr 00** - Bell Mobility, Nortel Networks, Qualcomm, Samsung y Sprint PCS culminan con éxito un conjunto de pruebas de llamadas inalámbricas de tercera generación, utilizando la tecnología 1X. **Abr 00** - La Asociación de la Industria de Información de EEUU (TIA) aprueba para publicación el estándar CDMA para módulos de identificación del suscriptor (tarjetas Subscriber Identity Module (SIM)). **Abr 00** - Lucent y Qualcomm completan primera transmisión de datos a 153 Kbps, con estándar CDMA Tercera Generación. **Abr 00** - Verizon Wireless anuncia

inversión de más de $ 3,000 millones de dólares en redes para el 2000. **May 00** - cdmaOne llega a más de 57 millones de suscriptores en todo el mundo. **Jun 00** - La australiana Telstra y Nortel completan la primera transmisión de datos con sistemas de tercera generación CDMA. **Jun 00** - CDG presenta al mercado mundial la tecnología 1xEV. **Ago 00** - CDMA continúa su expansión: 65 millones de usuarios. **Oct 00** - Más de 71 millones de usuarios seleccionan CDMA para sus comunicaciones móviles.

1.6.2. Resultado evolutivo de CDMA

La Unión Internacional de Telecomunicaciones (UIT) estableció sus especificaciones Internacionales para Telecomunicaciones Móviles 2000 (IMT-2000) con el fin de alcanzar un conjunto mundialmente armonizado de normas de Tercera Generación. Los sistemas de Tecnología de Transmisión de Radio compatibles con IMT-2000 proporcionan un vínculo estandarizado entre la red y el usuario, tanto para la tecnología de radio terrestre como satelital, para usuarios fijos y móviles de redes públicas y privadas.

Se presentaron una serie de propuestas para IMT-2000 a la UIT durante 1998. Desde entonces, la industria y los organismos de normas coordinaron sus esfuerzos para armonizar los candidatos a IMT-2000 y llegar a un conjunto más reducido de normas.

Cdma2000 posee tres fases de implementación para permitir la pronta instalación de la nueva tecnología, este enfoque permite a los operadores introducir más capacidad para servicios de voz junto con incrementos en la velocidad de los datos en intervalos que coinciden con la demanda emergente del mercado. Cdma2000, también incorpora Mobile IP, lo cual brinda a los usuarios móviles un acceso transparente a Internet e intranets de las empresas.

A fin de facilitar la migración de cdmaOne a las capacidades de cdma2000, ofreciendo características avanzadas en el mercado de una manera flexible y oportuna, su implementación se ha dividido en dos fases evolutivas.

> **Fase 1:** Las capacidades de la primera fase se han definido en una norma conocida como 1XRTT. La publicación de la 1XRTT se hizo en el primer trimestre de 1999. Esta norma introduce datos en paquetes a 144 kbps en un entorno móvil y a mayor velocidad en un entorno fijo. Las características disponibles con 1XRTT representan un incremento doble, tanto en la capacidad para voz como en el tiempo de operación en espera, así como una capacidad de datos de más de 300 kbps y servicios avanzados de datos en paquetes. Adicionalmente extiende considerablemente la

duración de la pila y contiene una tecnología mejorada en el modo inactivo. Se ofrecerán todas estas capacidades en un canal existente de 1.25 MHz de cdmaOne.

Fase II: La evolución de cdmaOne, hasta llegar a las capacidades completas de cdma2000, continuará en la segunda fase e incorporará las capacidades de 1XRTT, apoyará canales de todos los tamaños (5 MHz, 10 MHz, etc.), proporcionará velocidad de circuitos y datos en paquete de hasta 2 Mbps, incorporará capacidades avanzadas de multimedia e incluirá una estructura para los servicios de voz y codificadores de voz 3G, entre los que figuran los datos de paquetes de "voice over" y de circuitos. Los operadores podrán ofrecer datos y voz simultáneos, con velocidades de datos superiores a los 2,4Mbit/s, con cdma2000, 1xEV-DV. Cada uno de esos pasos evolutivos se proporciona dentro de sólo 1,25MHz de espectro. Cdma2000, parte del legado de la tecnología cdmaOne para ofrecer servicios de datos eficientes y gran capacidad de voz en una cantidad mínima de espectro (1.25MHz). Está diseñado para operar en una cantidad de bandas de frecuencia, inclusive las bandas celulares y las bandas PCS actuales, con incorporación de la flexibilidad a 2GHz también

1.7. Tecnología de radio IMT-2000

Aunque definidas dentro de un marco global, varias interfaces de radio han sido adoptadas para el móvil Tercera Generación. Esto fue necesario ya que, incluso después de largas discusiones, no todo el mundo involucrado pudo llegar a un acuerdo sobre una interfaz radio única debido a diferentes razones de tipo político, histórico y técnico

IMT-2000 es un estándar de la ITU definido por un grupo de recomendaciones de la serie M, F, G y Q. Agrupa una familia de sistemas con capacidades y servicios para la Tercera Generación. Extendida sobre la base de Sistema de Tercera Generación viene a consolidad y unificar los diversos e incompatibles ambientes móviles de hoy a una infraestructura de red y radio capaz de ofrecer un amplio rango de servicios a escala global. Barca una gama de servicios y terminales móviles enlazados a redes terrenas o satelitales y las terminales pueden ser diseñadas para uso móvil o fijo.

La ITU comenzó el camino de la estandarización de IMT-2000 cuando estableció el Interim Working Party 8/13 en 1985. Esta iniciativa fue llamada Future Public Land Movil Telecommunications Systems (FPLMTS), que en 1996 fue denominada como IMT-2000. En 1998 la ITU denominó Radio Transmision Techonology (RTT) a las tecnologías que harían

de interfaz aire entre las estaciones base y las terminales móviles. En junio de ese año, la ITU había recibido 15 propuestas, 10 terrestres y 5 satelitales. Las especificaciones técnicas de las RTT terrestres fueron aprobadas en la WRC-2000 y quedaron definidas como siguen:

- IMT-2000 CDMA Direct Spread (UTRA W-CDMA)
- IMT-2000 CDMA Multi-Carrier (cdma2000)
- IMT-2000 CDMA TDD (Utra TD-CDMA)
- IMT-2000 TDMA Single-Carrier

En la Conferencia Mundial de Radio WRC-92 se definió un rango de 230 MHz de espectro radioeléctrico, sin asociarlo a ninguna tecnología, en las bandas de 1885-2025 MHz y 2110-220 MHz identificadas para los servicios públicos IMT-2000, incluyendo las componentes por satélite y terrestres. Las bandas para la componente satelital de estos sistemas están comprendidas entre 1980-2010 y 2200 MHz.

Finalmente, en la WRC-2000, se aprobaron los requerimientos de espectro adicionales para la IMT-2000, la decisión proporciono 3 bandas:

- Banda 1 GHz (806-960 MHz).
- Banda 1.7 GHz (1710-1885 MHz). Frecuencia en la que funciona actualmente la mayoría de los sistemas de segunda Generación para facilita la evolución con el tiempo de estos sistemas a la Tercera Generación.
- Banda 2.5 GHz (2500-2690 MHz). Estas frecuencias completan la banda de la gama a 2 GHz ya identificada para IMT-2000.

Los sistemas de tercera generación deberán ofrecer:

- Uso de ancho de banda dinámico.
- Velocidades binarias muy altas de 144 kbps en alta movilidad, 384 kbps para espacios abiertos y de 3 Mbps para baja movilidad.
- Soporte para conmutación de paquetes (IP) como de circuitos.
- Transmisión simétrica/asimétrica de alta fiabilidad.
- Soporte de IP para acceso a Internet.
- Diferentes servicios simultáneos en una sola conexión.
- Soporte radioeléctrico flexible, con utilización más eficaz del espectro, con bandas de frecuencias comunes en todo el mundo.

Las distintas interfaces aire propuestas ante la UIT están basadas en CDMA que se acompañan de tres modalidades de operación, cada una de las cuales podrían funcionar sobre la red base de GSM (GSM-MAP) y sobre la red base de cdmaOne (IS-41)

En el caso del CDMA, los bits de información del usuario están distribuidos sobre un ancho de banda ampliado artificialmente, multiplexándolos con un flujo de bits con una tasa de bits seudoaleatoria más alta. Los bits en el flujo de bits seudoaleatorio, normalmente llamado código disperso, son referenciados como chips. Esta operación aumenta el ancho de banda que ocupaba la información original. La relación de la tasa del chip con la tasa de información original se llama ganancia de dispersión. Por sí misma, la dispersión del espectro no aporta ningún beneficio. Es la combinación de dispersión con la ausencia de ésta, incluyendo todas las técnicas avanzadas de procesamiento de la señal implantadas en el receptor, lo que hace que el CDMA sea atractivo. Una de las principales razones es que los mismos juegos de frecuencias pueden ser usados por cada una de las estaciones base de una red, debido a que cada conexión está asignada a un código de dispersión diferente. Una segunda razón tiene que ver con su capacidad para resolver caminos de propagación diferentes, convirtiendo la distorsión del camino múltiple en una buena aliada en vez de ser una molestia destructiva. Para ayudar a entender esta idea, conviene recordar que el FDMA evita que las conexiones de usuario puedan interferir unas con otras asignándoles distintas bandas de frecuencia. Mientras que los sistemas TDMA hacen esto por medio de la asignación de distintas ranuras de tiempo. Cuando se usa CDMA, las conexiones de usuario usan las mismas ranuras de tiempo y bandas de frecuencia, pero se distinguen unas de otras por los diferentes códigos de dispersión. En la operación de agrupamiento (no dispersión) se extraen todas las señales de interés. Las otras señales multiplexadas con códigos de dispersión diferentes simplemente se añaden al ruido de fondo, lo cual limita el número de usuarios que pueden compartir un canal.

Para que el sistema funcione, las potencias transmitidas deben controlarse estrictamente de tal manera que las señales desde todas las terminales móviles lleguen a la estación base con, aproximadamente, la misma potencia (igualmente para el enlace descendente) a pesar de sus distintas distancias a la estación base y a las diferentes condiciones de propagación. El bucle de control de potencia realiza medidas en el móvil y en la estación base. Los canales de control usados para informar de las medidas operan entre 800 Hz y 1,5 KHz.

Capítulo 2

Panorama para la protección de la Propiedad Intelectual de los Contenidos Digitales.

2. Panorama para la Protección de la Propiedad Intelectual de los Contenidos Digitales.

2.1. Antecedentes.

La legislación sobre patentes y derechos de creación de copias ha marcado el desarrollo de la tecnología informática. Hasta finales de los años 1960 el software era libre. El código fuente de los programas se distribuía sin inconvenientes entre los compradores de computadoras como parte del servicio que recibían, para que los utilizaran libremente y sin ningún costo adicional. En esa época, en las universidades fluía el código fuente de manera natural.

A principios de 1970 el panorama cambió drásticamente. La venta de software sin código fuente y sin permiso de redistribución ha marcado los últimos 30 años, situando entre las primeras del mundo por capitalización a empresas cuya fuente de ingresos casi exclusiva proviene de la venta de copias de software propietario.

La legislación sobre los derechos de copia se ha utilizado durante varios siglos no sólo para permitir el proteccionismo en ella, sino también en otras industrias más «clásicas», como la discográfica, la del vídeo y la editorial. En general, podría decirse que hasta la fecha las industrias de la información han tratado de impedir, con éxito, el flujo libre de información.

Por otro lado, cada vez son más voces las que reclaman una revisión de la legislación sobre patentes y los derechos de copia. La posibilidad de intercambiar datos con costo prácticamente nulo, gracias a Internet es considerado, en gran parte la razón con la que se está guiando este proceso de revisión que afecta a uno de los principales sectores económicos de las sociedades desarrolladas.

Podría marcarse como hito histórico la liberación del código fuente del navegador de Netscape, en 1998. Desde ese momento el software libre ha irrumpido en grandes sectores la industria informática: fabricantes de hardware como Intel, Cisco o Sony utilizan software libre sobre sus procesadores. Dell, Compaq e IBM distribuyen GNU/Linux con sus equipos.

Aún así, está por ver si existe un modelo económico viable que posibilite que una parte importante del software desarrollado por la industria se distribuya como software libre.

No sólo el software quiere ser libre, la distribución digital de información (audio, vídeo, libros) está alterando la industria tradicional.

2.1.1. Administración Tradicional de los Derechos de Autor.

Varias organizaciones de Derechos de Autor vienen trabajando ya, desde hace muchos años, en una etapa considerada como predigital, a este Sistema podemos bautizarle como Old

Rights Management (ORM). Todas estas organizaciones están ubicadas en Estados Unidos de Norteamérica.

El Copyright Clearance Center (CCC, www.copyright.com) desarrolló un sistema de licencia que permite a los usuarios de los materiales con derechos de autor cobrar las regalías para los editores. El CCC crea un sistema de administración de derechos efectivo, aunque sea un simple fotocopiado, siendo éste exitoso mucho antes de la llegada de Internet. Aunque el CCC inicialmente se dirige solamente, al fotocopiado de materiales de texto, el CCC exitosamente construye un sistema de Administración de Derechos.

Dentro de la Industria de la música, dos organizaciones han acordado el cobro de licencias de música en los Estados Unidos de Norteamérica: The American Society of Composers Authors and Publisher (ASCAP www.ascap.com) fundada en 1914 y la Broadcast Music Internacional BMI (www.bmi.com) fundada en 1940 ambas proporcionan un esquema al CCC durante el curso de su formación, una tercera organización el CESAC (www.cesac.com) se inició como una agencia de licencias para la música clásica en Europa, y recientemente ha empezado a representar a los compositores de música POP y a los editores en los Estados Unidos.

Dentro de la música, The Recording Industry Association of America (RIAA) funciona como un grupo de defensa para la industria de la grabación (www.riaa.com). Dentro de los miembros del RIAA se incluyen compañías que crean, fabrican y distribuyen aproximadamente el 90% de todas las grabaciones de sonido producidas y vendidas en los Estados Unidos.

En las películas se encuentran dos grupos: Motion Picture Association of America (MPAA) y The Motion Picture Association (MPA). El objetivo de estos grupos es girar incrementadamente a los derechos de la televisión, cable, video casero, y medios futuros de suministro de trabajos audiovisuales y aún los que no se han inventado.

2.2. Problemática.

Internet ha hecho posible que cualquier persona pueda intercambiar fácilmente información digitalizada con el resto de cibernautas.

El alcance global de Internet permite la transmisión de contenido a una escala sin precedentes. Al mismo tiempo, la tecnología digital "abundante y barata" hace posible: crear y, de manera eficiente distribuir todas las formas de los contenidos en un formato digital. El contenido, por consiguiente sin protección; es sumamente vulnerable a la estafa, al acceso no autorizado y a la propagación, ocasionando todo esto; grandes pérdidas financieras.

Por ejemplo, hace menos de dos años la industria musical se conmovió hasta la médula por un acrónimo pequeño pero poderoso: MP3. Este formato de archivo facilita al máximo la creación, distribución y compartición de archivos de música compacta con una fidelidad de sonido comparable a la que se encuentra en los Discos Compactos (CDs), ya que cualquiera podía grabar en el disco duro de su PC una canción de un CD en un archivo en formato MP3, y a través de la Organización Napster informar de la disponibilidad de ese archivo al resto del mundo. Unos minutos después alguien puede estar escuchando esa canción a miles de kilómetros. Esto alarmó tanto a la industria del sector que emprendió acciones legales contra la organización que los distribuye.

Fue como os estudiantes con experiencia tecnológica empezaron a comerciar ilegalmente colecciones de música copiadas a alta velocidad en Internet, y algunos artistas desconocidos explotaron el formato para que su música fuera oída por una gran audiencia sin tener que negociar con una discográfica. A las discográficas y a los artistas principales les encantaron las posibilidades de distribución instantánea, pero temían la amenaza de la piratería desenfrenada.

2.3. Como hacer frente a esta situación.

De manera simultánea a esta tendencia, la industria está tratando de emplear un amplio número de métodos técnicos y legales para impedir este proceso liberalizador: como por ejemplo libros electrónicos intransferibles que permiten sólo un cierto número de lecturas, mejoras en los códigos de protección en DVDs, una nueva legislación como la Uniform Computer Information Transaction Act (UCITA), un proyecto de ley que regula los contratos relacionados con la información digital. EE.UU pretende proporcionar un código normativo unificado que proteja las transacciones que involucren intercambios de programas e información, o aplicación estricta de la existente, como la persecución policial

Es notable, y como mínimo un hecho sobre el que vale la pena reflexionar, que a las primeras de cambio, en cuanto los medios técnicos lo han permitido, los ciudadanos opten en masa por copiar y dejarse copiar información, aun sabiendo que es ilegal. Y esto cuando la sociedad tiene (al menos teóricamente) una experiencia acumulada de cientos de años con la legislación de los derechos de copia en el sector del libro, y de casi un siglo en los sectores de grabaciones musicales e imagen.

Podría decirse que las personas tienen una tendencia natural a compartir la información.

Y por lo tanto, la sociedad tampoco ha podido experimentar nunca con las posibilidades que

proporciona el libre flujo de información (salvo en sectores concretos, y de forma parcial, como por ejemplo en el campo científico). Del enfrentamiento de estas dos fuerzas contrapuestas (por un lado las presiones para limitar el uso y distribución de la información, por otro las tendencias a usar y redistribuir información sin inconvenientes) dependerá el futuro, del acceso a la información digital en general, y posiblemente del mismo modelo de sociedad hacia el que nos dirigimos.

2.4. Empresas que proponen soluciones al uso no autorizado de contenidos digitales

Las compañías colaboran para ofrecer una Administración y distribución segura de materiales con derechos de autor en Internet, lo que significa una mayor libertad para los editores.

Dentro del mundo musical, varios grupos de esta industria y gigantes tecnológicos se unieron para crear la Iniciativa para la Música Digital Segura (SDMI), un esfuerzo para la administración de los derechos digitales (DRM) para proteger a los artistas y a los editores musicales de los peligros inherentes a la distribución en línea.

Varios productos y servicios ofrecen soluciones seguras amigables con el usuario, para proteger y distribuir contenido digital en Internet.

Entre estas compañías se encuentran:

Xerox Corporation (NYSE: XRX) y Microsoft Corp. (NASDAQ: MSFT) que unieron fuerzas para lanzar ContentGuard, Inc., compañía de Internet que ofrecerá soluciones integrales de software para proteger y administrar libros, documentos, música, software y otros contenidos valiosos distribuidos en la web.

El formato Windows Media de Microsoft ha incluido tecnología antipiratería en sus últimos lanzamientos. Esto significa que una compañía de discos que lanza una canción en este formato puede establecer reglas flexibles para su uso, lo que permite por ejemplo, que el consumidor escuche la canción un número ilimitado de veces o una sola vez, o que evite que el consumidor copie esa canción en un CD o en otra PC.

"Como una empresa que tiene compromisos fuertes en la electrónica y el entretenimiento, Sony con entusiasmo apoya la misión de la Iniciativa de Música Segura Digital, " Respetan los derechos de artistas y otros propietarios de derechos de autor y proporcionan una solución a la administración de los derechos de autor.

2.5. Pérdidas financieras.

En los últimos años, la distribución ilegítima de: música, películas, obras de arte, fotos, guiones y programas informáticos llamado más propiamente como contenido digital por

Internet ha sido un problema importante que ha causado pérdidas de millones de dólares en ingresos a los titulares de los derechos correspondientes.

Forrester Reserch estima que para el 2003 el mercado de transferencia (*download*) digital merecerá $2 mil millones de dólares americanos y el 25 % de ventas de música en línea serán transferencias (downloads) Pero la música en línea es un pequeño pedazo del pastel de contenido digital. Creemos que la mayor parte de contenidos de vídeo en el mercado se moverán al mercado de comercio dentro de 10 años.

Las investigaciones han puesto de manifiesto que la compensación del copyright o derecho de copia representa actualmente tan sólo un 10% del negocio potencial. Se pierden más de 20.000 millones de euros debido principalmente a la inexistencia de una infraestructura de cámara de compensación de derechos de propiedad intelectual en Internet.

La piratería en Internet ha crecido exponencialmente durante los dos años pasados. El pico mas alto fue en febrero 2001, donde aproximadamente 2.8 mil millones de canciones habían sido comerciadas por Napster.

La International Federation of the Phonographic Industry (IFPR), informa que han decrecido sus ventas de singles en el año 2000 de un 14.3% de 439 millones de unidades a 376 millones.

2.6. Importancia de tener una Administración de Derechos Digitales (DRM)

La tecnología DRM ha sido desarrollada para proteger el comercio, la posesión de la propiedad intelectual, y la privacidad de los derechos de los creadores de contenidos digitales. La cadena de valor esta compuesta por el creador, distribuidor, consumidor, y, hasta aún más lejos, del consumidor a otros consumidores.

DRM protege y trata el contenido basado en reglas de uso especificadas por los dueños de contenidos y los poseedores de los derechos.

DRM puede ser usado también para controlar y rastrear el acceso autorizado y para el control en la comercialización, ventas, derechos y penetración. Para estos motivos, DRM puede ser un componente importante en la estrategia de negocio de una organización. Los diferentes tipos de organizaciones pueden tener motivos diferentes para la protección y el tratamiento o manejo de sus contenidos digitales.

Los dueños de Contenidos y proveedores de servicios pueden querer controlar el acceso a su contenido para generar ingresos de su venta, mientras una empresa puede querer compartir el contenido, pero no venderlo.

Las corporaciones generalmente implementarán DRM para uno de dos objetivos primarios:

- DRM para comercio: Este es el empleo de DRM para proteger el valor monetario del contenido digital protegiéndolo del empleo no autorizado e implementando términos y condiciones de pago asociadas con el empleo autorizado, legítimo.
- DRM para confidencialidad. También conocido como DRM para privacidad, esto es el empleo de DRM para proteger la confidencialidad de información - para protegerlo del empleo no autorizado, para manipular la manera en que esto puede ser usado sobre una base autorizada, y posiblemente registrar cuándo y cómo esto es usado.

Una empresa dada de hecho puede tener ambas necesidades de comercio y de confidencialidad para las diferentes partes de su negocio.

En el sentido más básico, el contenido es una propiedad intelectual. En la empresa cualquier clase de información o de propiedad intelectual puede ser un contenido; sin embargo, esto generalmente es mencionado como "información" en vez de "contenido".

En el caso en el que el contenido o sea la información sea independiente de su formato. Justo es el caso en que puede existir como un libro, como una grabación, o como un video y continuar siendo el mismo caso, entonces es el contenido el producto de la creatividad, y el ámbito de estudio es la propiedad intelectual. Los formatos (por ejemplo, PDF, JPEG, MPEG2, y MP3) son los transportadores de contenido.

En el caso de Operadoras de Comunicaciones Móviles, con la implementación de 2.5 G y Tercera Generación (3G) estudiada previamente, se crearán nuevos canales para la distribución y venta de contenidos digitales y de acceso a la información. Esto les proveerá una oportunidad única a los proveedores de contenidos que generará otra cadena de ingresos para sus contenidos. Sin embargo esto tiene un problema asociado; los contenidos digitales no protegidos serán vulnerables al robo, acceso y distribución no autorizada.

2.7. Nuevos Negocios, Nuevas Posibilidades

Los nuevos caminos de la distribución de contenidos, ya sea en línea o fuera de línea, están basados en los modelos de negocio.

Un cuestionamiento importante es el tamaño del contenido que se deberá vender, ya que en Internet le permite vender cualquier tamaño de contenido.

A continuación se describirán modelos de negocio su relación y aplicación en DRM.

2.7.1. Pago de Download (transferencia).

En el download cuando se accede a un sitio Web, se deberá llenar una solicitud con la información que el proveedor solicita, se deberá ingresa el numero de la tarjeta de crédito, y entonces se podrá obtener un archivo en forma encriptada, también se obtiene una aplicación cliente que desencripta el contenido lo reproduce y/o lo muestra, o lo transfiera a otra aplicación. Este un uno de los pocos modelos de negocio que es anterior a los sistemas DRM.

El Pago por transferencias no es una mala idea, y el modelo de negocio le da sentido porque esto es una analogía directa del comercio de artículos físicos. Por ejemplo, vas a una librería y compras un libro, vas a un sitio Web y compras una pieza de contenido, el pago por las transferencias o descargas se aproxima a el primer ejemplo de negocio y la tecnología DRM hace esto posible, aproxima los modelos de derecho inherentes a las compras de contenidos físicos de esta naturaleza. En el existen dos pequeñas complicaciones:

- Es complejo comprar el contenido, es aún más complejo el uso de la tecnología DRM.
- La gente no esta acostumbrada por ejemplo a leer libros confortablemente en su PC o portátil.

Es importante, que no se examine mucho el primer punto, la barrera para comprar el contenido es el proceso no el precio.

El pago del modelo de transferencia, al equivalente digital de un libro de un CD o de un video en un establecimiento comercial, eventualmente tienen modelos de negocio con DRM en Internet, es más usado para trabajar con un valor elevado, obtener un contenido en un tiempo crítico que no esta disponible desde otra fuente, o como una alternativa a los sistemas de suscripción de aquellos usuarios que quieren solo pruebas pequeñas del contenido que se esta ofreciendo.

2.7.2. Suscripciones.

El modelo de suscripción tradicionalmente ha sido en línea, se firma una suscripción y se proporciona el nombre del usuario y el password el cual proporciona el acceso, solamente a aquellos suscriptores de un sitio Web, no previene el copiado del material que se encuentra y que se envía a una serie de usuarios. En una empresa, donde el contenido es compartido, pero no vendido, el acceso generalmente es controlado por autenticación usuario/ contraseña. Esto, sin embargo, no controla la política o lo que los usuarios pueden hacer con el contenido una vez que ellos ya tienen el acceso.

2.7.3. Pay-Per-View y Pay-Per-Listen

El *Pay-Per-View* es posiblemente el modelo de negocio más viejo para el contenido en el mundo físico, se aplica para eventos tales como conciertos, juegos y para películas con la condición de no volver a ver la película una segunda vez, siendo trasladado a el mundo digital, donde se pagara por ver cierto evento solamente una vez.

El *Pay-Per-Listen* en el mundo físico es aplicado en las rockolas, en algunos establecimientos de diversión.

2.7.4. Superdistribución.

La superdistribución, es una distribución de etapas múltiples es decir, se transfiere un objeto más de una vez, en realidad la mayoría de los contenidos en el mundo, están a través de etapas múltiples en la distribución. Se refiere a una distribución múltiple del mismo archivo digital, y más típicamente se refiere al *peer-to-peer*.

Capítulo 3

Digital Rights Management DRM. (Administración de Derechos Digitales)

3. Digital Rights Management DRM. (Administración de Derechos Digitales)

Con el propósito de asegurar que los consumidores paguen por la utilización de contenidos digitales y que los proveedores de contenidos sean suficientemente remunerados. DRM tiene la intención de controlar el acceso y el empleo de contenido digital. Esto puede ser implementado poniendo en práctica varias medidas tecnológicas de protección.

La Administración de Derechos Digitales (ADD) o en inglés DRM promete ofrecer un marco seguro para la distribución de contenidos digitales. DRM permite a un mercado electrónico donde el modelo antes inimaginable de negocio puede ser puesto en práctica. Al mismo tiempo, DRM asegura que los proveedores de contenido en particular los dueños de derechos de autor reciban la remuneración adecuada por la creación de contenido que es distribuido sobre DRM.

Las técnicas de cifrado son sobre todo importantes; los "contenedores digitales" permiten el cifrado duradero de distribución de contenido. Las tecnologías de control de copiado como es "Copy Generation Management System" (CGMS) usado en reproductores DVD o el "Serial Copy Management System" (SCMS) usado en DAT y reproductores de Minidisco controlan el número de las copias de contenido digital que un usuario es capaz de hacer.

DRM puede emplear varios medios que impiden o responde activamente a brechas de seguridad. Los filtros Especializados y la tecnología de marcas de agua o un robusto *hash* pueden bloquear el acceso al contenido pirateado

3.1. Concepto de DRM

DRM es una cadena servicios y tecnologías de hardware y software que manejan el empleo autorizado de contenido digital y manejando cualesquiera de las consecuencias de su empleo a lo largo del ciclo de vida entero del contenido.

DRM es un sistema que permite a los propietarios de los contenidos digitales controlar el uso y la cantidad de copias que se hacen de sus trabajos.

La Administración de Derechos Digitales "o" DRM significa técnicas, procesos, procedimientos y algoritmos relacionados al establecimiento de un ambiente que utiliza sintácticamente oraciones declarativas que tienen un amplio entorno significativo para la Administración de derechos convertido en un formato digital, incluyendo el hardware y el software de los dispositivos

electrónicos, lo que permitiría o implementaría un licenciamiento confiable, derechos seguros y especificación de permisos, así como derechos y la ejecución de éstos, el establecimiento de un desarrollo de un residente o dispositivo, así como también una infraestructura fiables.

DRM crea y mantiene la existencia de servicios e infraestructuras fiables, las bases de un servicio es una alianza fiable, esto establece que cuando ambas partes entre (proveedor-vendedor y el receptor-cliente) puede confiar que el contenido que fue enviado es auténtico, y que fue enviado de quien se supone debía haber sido enviado, y que es accesible solo para los receptores contratantes bajos los derechos adquiridos.

La infraestructura fuerza a tener accesos y alianzas confiables, los servicios confiables son un requerimiento para una segura distribución de contenidos. Al mismo tiempo, los participantes del proceso están a la expectativa de un grado de control sobre los aspectos operacionales de su negocio. Consecuentemente, las tecnologías de una plataforma DRM deben proporcionar una flexibilidad para poder construir servicios confiables mientras les permite mantener el control sobre sus negocios.

La tecnología DRM trae transacciones seguras de comercio digitales, incluyendo la ejecución automatizada y persistente de política para un consumo de bienes digitales, siguiendo la pista, la detección de fraude, la Administración de accesos o de cuentas, la creación y administración de llaves o claves de cifrado y funciones similares, que se ejecutan sobre sistemas de distribución que son redes internas y externas.

DRM tiene 4 controladores principales de mercado:

- Protección a la Propiedad Intelectual.
- Nuevas oportunidades de ingresos.
- Protección de la privacidad y confidencialidad.
- Estándares para la Protección de contenidos.

3.1.1. Términos empleados en un sistema DRM

Contenido Digital: En el más básico de lo sentidos, el contenido es una propiedad o trabajo intelectual.

En la empresa, cualquier tipo de información o propiedad Intelectual puede ser un contenido; en cualquier caso el contenido es independiente de su formato.

Por ejemplo una historia puede existir como un libro, como una grabación o como un video y puede seguir siendo la misma historia.

Los contenidos pueden ser del tipo:

Texto: un conjunto de texto y otros activos asociados (como pueden ser imágenes) producidos como libros, documentos, cartas, seguridad de reportes, guías de localización, catálogos, libros de texto, formas, etc.

Audio: música, llamadas en conferencia, dictados, lecturas,etc.

Vídeo: películas, conferencias, procedimientos médicos, tours, demos, reuniones, etc.

Imágenes: fotos, mapas, rayos-x, informes de clima, huellas digitales, etc.

Otros datos: juegos de multimedia, software, etc.

Los formatos son la envoltura de los contenidos.

- **Poseedor o dueño de los derechos (*Rightsholder*):** Es una entidad legal, (persona o compañía) dueña de los derechos de una propiedad intelectual (copyright, trademark (marca), patente, etc.) posee un convenio para el uso de sus derechos.
- **Usuario:** Es una entidad legal que ejecuta como hacer uso de los derechos de una propiedad intelectual.
- **Dueños de Contenidos**: Un dueño de contenidos es un individuo o una organización que posee el derecho de reproducir y/ o distribuir un tipo de contenido. Esto puede incluir al autor o autores originales de un trabajo u organizaciones, como son libros y editores de música, que han adquirido los derechos del trabajo del autor original. Este es un término frecuentemente intercambiable con el poseedor de los derechos, podríamos decir que es impreciso ya que algunas veces el dueño del contenido no es el dueño de todos los derechos del contenido. Por ejemplo puede tener todos los derechos del contenido para una parte de América, y en la Unión Europea, solo algunos de éstos. El es sin embargo a quien se le refiere como el dueño del contenido.
- ***Cleringhouse* o Agente:** Una entidad legal (persona o compañía) autorizada por un *rightsholder* o dueño de los derechos para ingresar una transacción de derechos en lugar del dueño de los derechos, son entidades que realizan una forma más eficiente la transacción de los derechos.
- **Transacción de derechos:** Termino utilizado para determinar que tipo de operación se efectúa sobre los contenidos digitales, entre el dueño del contenido y el usuario final.
- **Regalías:** Una compensación monetaria para el poseedor o dueño de los derechos hecha por medio de su agente o *cleringhouse* por el uso de los derechos de su propiedad intelectual.

- **Distribuidores de contenidos**: Los proveedores de Servicios de Contenido entregan directamente al usuario final el contenido. Dentro de estos se encuentran los siguientes ejemplos: AOL Time Warner, Echostar, y Vodafone. Aunque el contenido sea entregado, la infraestructura es requerida o pretendida para la entrega del contenido directamente al usuario final o el consumidor.
- **Fabricantes de Dispositivos**: Los fabricantes de dispositivo son firmas comerciales de todos los tamaños que diseñan y producen dispositivos digitales. Los dispositivos varian extensamente en un factor de forma, funcionalidad, y inteligencia, en ellos se incluyen PCs, reproductores digitales de audio, teléfonos móviles, asistentes personales digitales (PDAs) La tecnología DRM puede ser desplegada dentro de los dispositivos para actuar recíprocamente y hacer cumplir derechos de los contenidos. Por ejemplo, DRM puede ser integrado con un chip, con el sistema operativo, aplicaciones, o una combinación de todos estos. Algunos ejemplos de fabricantes de dispositivo incluyen Nokia, Palm, Philips, RCA, y SonicBlue.

3.2. Arquitectura de un Sistema DRM

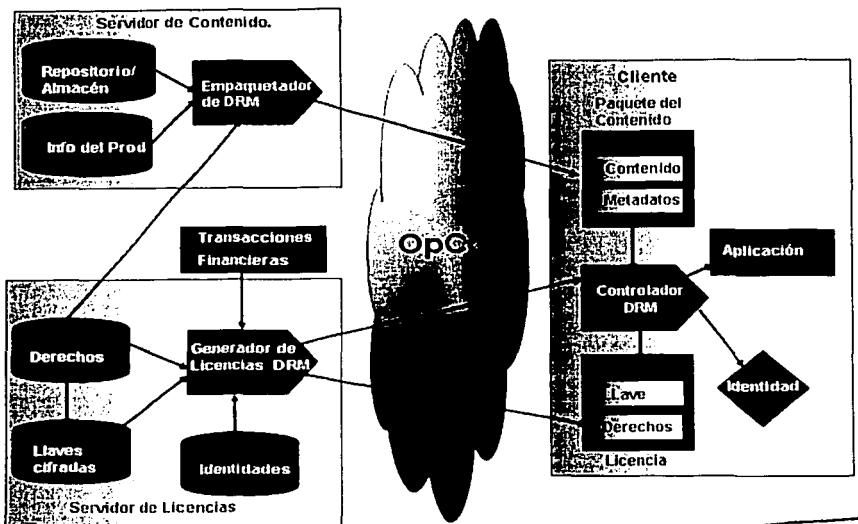


Figura 3.1 Diagrama a bloques de un Sistema DRM.

En el esquema anterior se muestra de una manera muy sencilla y general un ciclo completo de los contenidos digitales los cuales tienen asociados una tecnología de DRM. Cada solución de cada proveedor muestra algunas diferencias propias a la arquitectura aquí presentada.

Dos tipos de aplicaciones están presentes en un Sistema DRM, aquéllas que fueron creadas específicamente para sistemas DRM y las de propósito-general que un Sistema DRM modifica en función a las restricciones de su funcionamiento.

Se muestra un ciclo desde los dueños de los contenidos digitales hasta el consumidor final.

Un sistema DRM por lo general tiene cuatro componentes principales:

- El Servidor de Contenido.
- Una red de distribución de contenido y derechos asociados (Operadora de Comunicaciones OpCo)
- Un servidor expendedor de licencias.
- Software que será capaz de reproducir el contenido en el dispositivo del usuario.

A continuación se describirán cada una de las partes que conforman una arquitectura DRM.

3.2.1. Servidor de Contenido

En una arquitectura DRM se tiene un contenido, la información acerca de los productos (o servicios) que el proveedor del contenido busca distribuir, y funcionalmente preparara al contenido para una distribución segura basada en DRM.

3.2.1.1. Repositorio / Almacén de Contenidos Digitales.

Un Proveedor de contenido que implementa una solución DRM tiene un repositorio o almacén de contenido, el cual es una colección del contenido que están en un formato (MPEG4, PDF, WAV, etc.) para su posterior distribución a través de una red de comunicaciones.

El repositorio es frecuentemente construido dentro de una solución DRM o algunas veces tendrá una interfaz para una solución DRM, que sirve para múltiples propósitos. Muchos publicadores/creadores/dueños están construyendo sistemas que administren los contenidos que sirven a un conjunto de canales de distribución simultáneamente, tal como para imprimir y para una distribución regulada al cliente vía DRM.

Desde el punto de vista pragmático, un repositorio es un servidor de archivos o una base de datos, en cualquier de los casos se posee al contenido como también a los metadatos que son información acerca de los contenidos.

3.2.1.2. Empaquetador de DRM

Cada sistema DRM basado en cifrado contiene una funcionalidad que prepara al contenido para su distribución a través del sistema quién realiza esta tarea se le llama Empaquetador de DRM.

El empaquetador de DRM crea las descripciones de los derechos que el proveedor del contenido quiere permitirle al usuario para la ejecución de su contenido. La solución DRM permite al proveedor del contenido especificar derechos a través de una interfaz de usuario, a través de procesos batch, o a través de un programa hecho en C++ o Java y trabaja con componentes del servidor expendedor de licencia

El contenido empacado podrá existir como una unidad indivisible; alternativamente, el paquete podrá simplemente contener metadatos y un vínculo al contenido a través de un metadato de identificación.
Otro proceso del empaquetador de DRM consiste en la creación de un conjunto de llaves cifradas que serán usadas para la autenticación de los usuarios y el descifrado del contenido. El contenido es cifrado utilizando algoritmos de encriptación estándares como por ejemplo AES, DES, RSA, SHA-1

3.2.1.3. Información del Producto (Info del Prod)

Para un mundo físico los proveedores de contenido típicamente tienen catálogos de información de sus productos. Estos contienen metadatos acerca de los productos, como su precio, información de mercado, formato, dimensiones físicas y más. En una implementación DRM los proveedores de contenidos necesitan crear bases de datos de la información acerca de sus productos que intentan vender.
El contenido del paquete contiene metadatos. Hay varios tipos de metadatos, por ejemplo:

- **Identificación:** Un número único que el publicador o dueño del contenido le asigna a cada pieza de contenido el cual se puede usar como referencia para múltiples propósitos, como por ejemplo insertar información de la actualización del precio, para rastrear el uso de sus contenidos remotamente.
- *Discovery*: Información que le ayuda al usuario a localizar el contenido, como palabras claves, título y autor.

El contenido y los metadatos, ambos en un paquete, son usualmente cifrados. Aunque los metadatos no necesitan ser cifrados.

3.2.2. Una red de distribución de contenidos y derechos asociados (Operadora de Comunicaciones OpCo).

De una forma muy intuitiva de entenderlo, una red consiste en dos equipos conectados entre sí mediante un cable de tal forma que se pueda compartir la información. Todas las redes, no importando lo sofisticadas que sean, parten de esta sencilla idea.
Una red será más fiable si existen caminos redundantes, es decir, puede alcanzarse un destino a través de varias rutas. Si falla una de ellas, la red no queda inutilizada.

3.2.3. Servidor de Licencias.

Las Licencias contienen información acerca de la identidad del usuario o dispositivo que ejecutara los derechos de los contenidos, identificación de el contenido con lo cuál se le aplicaran lo derechos, que son especificaciones de los derechos de uso de la Propiedad Intelectual.

3.2.3.1. Modelado de derechos o especificación de Reglas de Uso.

En el modelo de los derechos se describen los tipos de derechos y atributos de esos derechos.
Se han esquematizado de la siguiente manera:

- **Derechos de Suministro:** Son los derechos que suministra el contenido o la representación de estos en algún medio especifico de salida. Hay tres tipos importantes de estos derechos: la **impresión** suministrada como una copia impresa, como **vista** mostrada en un visualizador, como la pantalla de una computadora, como una **reproducción** suministrando el contenido en secuencia desde el comienzo hasta el fin, antes de que el tiempo de suministro se termine.
- **Derechos de Transporte:** son los derechos para mover o copiar contenido de un lugar a otro, en la **copia** ambos usuarios tienen acceso simultáneo al contenido, **movimiento** el primer usuario da acceso después de moverlo a un segundo usuario, en el **préstamo** el primer usuario cede acceso al segundo, pero solamente temporalmente cuando el segundo usuario proporciona los derechos al contenido devuelto. No hay más acceso aunque el primer usuario lo tiene nuevamente, no hay un acceso simultáneo.
- **Derechos Derivados:** Son aquellos que se hacen con la manipulación de los contenidos, para la creación de trabajos adicionales (derivados), como la **derechos de extracción** son los derechos que usan piezas de contenidos de su creador, como el capítulo de un libro, **derechos de edición** son aquellos derechos para cambiar algo de un contenido a cualquier otra cosa, **derechos para embeber** son los derechos para obtener una pieza de un contenido y usarlo completamente en un diferente contenido.

Los atributos de los derechos son una parte importante del modelado de derechos, estos son particularmente adjuntados a cada uno de los derechos fundamentales. Son tres los términos importantes de los atributos de los derechos que considerare:

- La **extensión** este de define como el tamaño, el número de veces, o en que lugar se aplican los derechos, por ejemplo: obtener 500 re-impresiones de un artículo de revista, uso de un producto en una versión de prueba por 30 días.

- La **remuneración** con todo lo que el usuario tiene que compensar por unos derechos, en otras palabras el tipo de remuneración es el dinero, pero esto puede ser cualquier cosa de valor para el publicador o dueño.
- Los **tipos de usuario** permite especificar diferentes conjuntos de derechos y atributos para diferentes clases de usuarios, por ejemplo, puede hacerse que el contenido este disponible a un bajo costo para estudiantes.

Así las reglas pueden ser definidas por un rango de criterios, los cuáles incluyen: precio (¿Cuánto se va ha pagar por el conjunto de derechos para este contenido?), duración (Ejemplo: ver el contenido por un año, por un mes por tres horas), frecuencia de acceso ejemplo (utilizarlo solamente una vez, escucharlo por 10 veces) versión (Puede ser salvado, copiado, almacenado en un CD, o impreso, y las veces que se pueda permitir), transferencia (ejemplo: puede ser re-enviado o transferido a otros usuarios o dispositivos).
Las reglas pueden ser combinadas para forzar varios modelos de negocio, incluyendo la suscripción pago por evento, promoción, superdistribución, licencias temporales.
Las soluciones más sofisticadas de DRM contienen formas flexibles, de expresar estos derechos. Como pueden ser lenguajes específicos para derechos como el extensible Rights Markup Language (XrML) algunos usan conjuntos de rutinas del lenguaje de programación en C++ o Java.

3.2.3.2. Generador de Licencias

Se obtendrán licencias DRM que darán acceso a una pieza especifica de contenido, estas licencias tendrán acceso únicamente a una pieza de la colección de los contenidos sobre un cierto periodo de tiempo.
El servidor de licencia también almacena identidades, que es información acerca de los usuarios que ejecutaran los derechos del contenido, todas estas identidades serán suficientes para que el generador de licencias las genere y las envíe a los usuarios.
Existen muchas maneras para la implementación de licencias, cada proveedor, proporciona diferentes soluciones.

3.2.3.3. Identidades, especificaciones de derechos y llaves de cifrado.

Un usuario tiene que establecer una identidad para ser claro en el empleo de los derechos de los contenidos. La autentificación de identidades es una de los clásicos problemas en el campo de la seguridad. Surge una discusión ¿qué es lo que se debe de identificar al usuario o al dispositivo?, ya

que por ejemplo un usuario puede buscar la forma de ver o reproducir un contenido en múltiples dispositivos como el dueño, podría querer leer un libro electrónico en una PC y en una PDA.
La identidad de un usuario deberá tener:

- Información proporcionada por el usuario como: el nombre, e-mail, dirección, número telefónico, número del Seguro Social, un identificador de usuario o *password*.
- Información inherente al usuario como: huellas digitales, rastreo de la retina ocular.
- Información del usuario proporcionada por terceras partes fiables como: un certificado digital.

Cada tipo de identidad tiene sus pros y sus contras. En general, todas esas piezas de información son fácilmente transferibles de una persona a otra, haciendo que el valor principal de autentificar sea únicamente una aproximación.
La autentificación de identidades de dispositivos, de manera simple es identificando al dispositivo colocándole un numero serial y que el software pueda leer. Intel esta intentando hacer esto con algunos de sus microprocesadores.
La especificación de los derechos y las llaves son almacenadas en bases de datos separadas para una mayor seguridad. Cada una de estas bases de datos contiene únicos identificadores que vincula a los derechos y a la llave a cada contenido en particular.

3.2.4. El cliente.

El cliente es un conjunto de entidades y es realmente la combinación del usuario y el dispositivo que esta usando (*handset* o PC).

3.2.4.1. El Controlador DRM

En nuestro esquema puede observarse como una pieza independiente de software, sin embargo puede residir en la aplicación (reproductor, visualizador) o puede ser únicamente una pieza de hardware.
Dentro de sus funcionalidades se encuentran:

- Recibir la solicitud del usuario para ejecutar los derechos sobre un paquete de contenido.
- Reunir la información de la identidad del usuario y obtener una licencia desde el servidor expendedor de licencias.
- Recuperar la llave descifrada de la licencia, descifrar el contenido y liberarlo para que lo reproduzca la aplicación.
- Autenticar la aplicación que realiza la ejecución de los derechos.

3.2.4.2. El Contenido del Paquete

El contenido y los metadatos, ambos en un paquete son usualmente cifrados. Aunque los metadatos no necesitan ser cifrados. El contenido empacado podrá existir como una unidad indivisible; alternativamente, el paquete podrá simplemente contener metadatos y un vínculo al contenido a través de un metadato de identificación.

3.2.4.3. La Licencia.

Es una pieza de contenido, emitida por el servidor de Licencias, el cuál contiene la llave con la cuál se podrá descifrar el contenido y los derechos lo cuales ejecutaran la pieza de contenido para su reproducción.

3.3. Secuencia de eventos de un Sistema DRM.

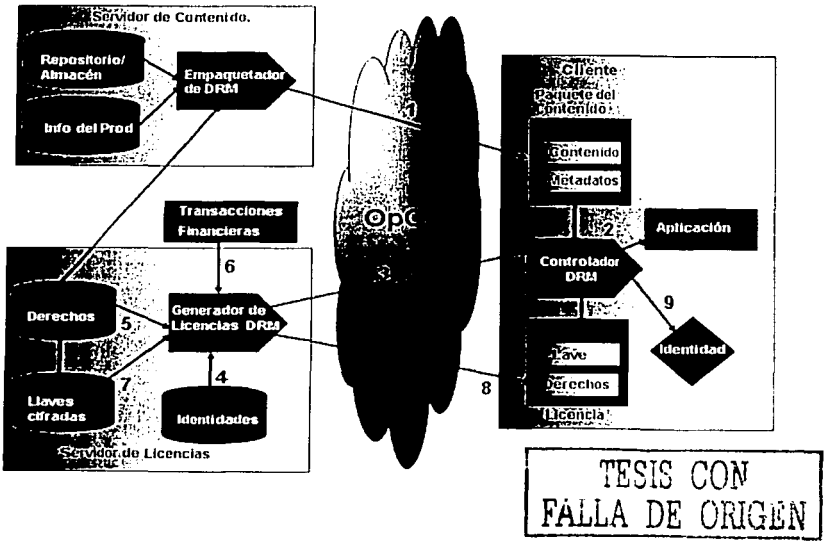


Figura 3.2 Secuencia de eventos en un Sistema DRM con la ejecución de los derechos asociados al contenido.

El primer suceso es cuando un usuario obtiene un paquete de contenido, el cual fue obtenido de diferentes formas (1), como *downloading* (transfiriendo) desde un sitio Web o de un servidor File Transfer Protocol (FTP) o separándolo de un mensaje de e-mail, o leyéndolo desde cualquier medio físico como un CD-ROM. En el mismo punto después el usuario obtiene el paquete de contenido, se hace una solicitud para ejecutar los derechos en el paquete (2) el usuario realiza esto mediante la selección de un opción en el menú en la aplicación ejecutando un comando de el sistema operativo, o haciendo *double-click* en un archivo, o haciendo que genéricamente se active el controlador de DRM. Una vez activado el controlador DRM reúne la información necesaria para generar la licencia y también la obtención de la información de la identidad del usuario y/o dispositivo del cliente y la

Esto será que el usuario llene una forma de registro (posiblemente contenga un número de una tarjeta de crédito) o también presionando el botón donde acepte un acuerdo de licenciamiento el usuario final. Después de que se haya creado la identidad se pasa al Servidor de Licencia para la inserción en la base de datos de identidades.

El Controlador DRM del cliente entonces envía la identidad y la información del contenido en una solicitud al servidor de licencia **(3)**. El generador de licencia autentifica la identidad del cliente contra la base de datos de identidades **(4)** y usa el identificador del contenido para observar la información de los derechos acerca del contenido **(5)**. Entonces luego este reúne la información de los derechos de la licencia del usuario solicitada. Si es necesario, este arranca una transacción financiera en este punto **(6)**. Finalmente, el generador de licencias capta la información de los derechos, junta la información de la identidad del cliente, y las llaves de encriptación **(7)**, y crea una licencia, la cual es por si misma encriptada o al menos a prueba de falsificaciones, esta es enviada nuevamente al cliente. **(8)** En este mismo punto de este proceso. El controlador de DRM en el lado del cliente puede tener etapas para autentificar la aplicación dada que hará seguramente que esta sea autorizada para ver el contenido. Después de que la licencia es generada y los pasos de autentificación son completados, el Controlador de DRM podrá descifrar el contenido obteniendo la llave de la licencia que le ha sido enviada y lo actualiza dentro de la aplicación **(9)**. Finalmente la aplicación reproducirá o mostrara el contenido al usuario en función de las reglas de uso que se hallan definido para dicho contenido.

Capítulo 4

Herramientas Utilizadas para la Protección de Contenidos Digitales

4. Herramientas Utilizadas para la Protección de los Contenidos Digitales.

El cifrado es una tecnología central para DRM, muchas de las discusiones constantes acerca de la eficacia de los sistemas DRM para la protección de copia y reproducción de los contenidos, se enfocan en el poder del cifrado aún pensando que en la mayoría de los ejemplos, en donde los sistemas DRM puedan ser craqueados no desarrollan el rompimiento del cifrado actual, si no en su lugar, se han desarrollado nuevos algoritmos para una mayor seguridad.

4.1. Técnica de Cifrado.

La encriptación o cifrado es la codificación de los datos para ocultar su contenido a todo el mundo excepto al receptor indicado. Los algoritmos matemáticos utilizados para cifrar los datos se denominan cifrados.

Algunas Definiciones:

- **Mensajes** denotado por **M**: palabras o sucesiones finitas de letras o elementos de un cierto Alfabeto (finito) A (español, binario, etc).
- **Cifrado**: Para garantizar el secreto de M, el emisor lo transforma en otro mensaje C (aparentemente sin sentido), empleando un Código Secreto o Sistema Criptográfico.
- **Descifrado**: El receptor recupera M mediante una operación descifrado inversa de la anterior.
- **Sistema Criptográfico o de Cifrado: (M, C , K):**

  M conjunto de mensajes originales (o en claro);

  C conjunto de mensajes cifrados;

  K conjunto finito de llaves (o claves);

junto con dos aplicaciones:

$$c : M \times K \rightarrow C \quad \text{y} \quad d : C \times K \rightarrow M$$

tales que $d(c(M, k)) = M$ para todo $(M, k) \quad M \in K$.

- **Los mensajes en claro** $M \in$ M son sucesiones finitas de símbolos de un cierto alfabeto A. La operación de cifrado c(M, k) del mensaje M con la clave $k \in K$

produce un nuevo mensaje $e(M,k) = C$ que normalmente supondremos que también está escrito en el alfabeto A. El mensaje cifrado se recupera mediante la función de descifrado.

Una función de cifrado debe ser tal que con ella obtener las imágenes en el código de los elementos del alfabeto fuente sea un proceso simple y rápido, pero la operación contraria, obtener elementos del alfabeto fuente a partir de sus imágenes en el código, si no se conocen ciertos datos (como la llave o la clave) debe resultar lo más complicado posible. Ese es el verdadero sentido de una buena función de cifrado.

La inclusión de las llaves en los procesos de encriptación y desencriptación se realiza introduciendo las mismas en los procesos matemáticos pertinentes, generalmente como constantes en la función de codificación. Cuánto más longitud tenga la clave usada, más seguro será el sistema de encriptación y más difícil será romperlo por criptoanálisis, aunque esta fortaleza del cifrado también depende del sistema en sí.

Un sistema de cifrado, para considerarlo *seguro*, necesita tener cuatro características o funcionalidades:

- **Confidencialidad**: el contenido de la comunicación ha de ser inútil para una tercera persona que lo pudiera interceptar.
- **Autenticación**: el sistema debe asegurarnos que una tercera parte no puede usurpar la identidad de alguna de las dos partes que intervienen en la comunicación.
- **Integridad**: nos debe garantizar que la información transmitida, además de no ser interceptada, no pueda ser modificada por una tercera parte.
- **No repudio**: debe garantizar que ninguno de los participantes en una comunicación pueda negar parte de la misma.

La criptografía convencional nos ofrece dos alternativas al problema del cifrado en las comunicaciones: la criptografía simétrica y la criptografía asimétrica o de clave pública.

4.1.1. Criptografía simétrica

Es el sistema de cifrado más antiguo y consiste en que tanto el emisor como el receptor cifran y descifran la información con una única clave que ambos comparten. El emisor cifra el mensaje con la clave secreta y se lo envía al receptor. Este último, que conoce la clave secreta, la utiliza para descifrar la información.

Este sistema de cifrado tiene la ventaja de ser altamente eficiente, dado que los algoritmos utilizados son muy rápidos. Su mayor inconveniente, es que la clave secreta, al ser compartida, ha de ser comunicada de forma segura entra las dos partes implicadas en la comunicación (por teléfono, correo certificado, etc.).

En la siguiente figura se puede observar un ejemplo del funcionamiento de la criptografía simétrica.

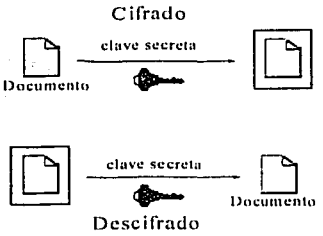


Figura 4.1 Algoritmo Simétrico de clave Secreta.

4.1.1.1. Algoritmo DES (Data Encryption Standar)

A la criptografía simétrica pertenecen los cifradores de bloques, los cifradores de flujo y las funciones 'hash'. De los cifradores de bloques (se llaman así porque cifran de bloque en bloque de 64 bits), podemos citar al famoso Data Encryption Standar (DES); actualmente, se usa una versión más robusta, denominada Triple-DES (consistente en aplicar tres veces DES). A lo largo de los años se han propuesto una cantidad considerable de algoritmos, que sin embargo no han tenido tanta aceptación, como lo es el caso del estudio DES.

Este algoritmo de Cifrado de Bloque fue creado el 15 de mayo de 1973 y adoptado en agosto de 1974 por NBS (ahora llamado NIST Instituto Nacional de Estándar y Tecnología) como algoritmo de encripción de seguridad para uso de aplicaciones gubernamentales.

Fue adoptado por el gobierno Federal de US como un estándar en el año de 1976. Fue publicado por el NBS como único hardware en un Proyecto realizado en el año de 1977 y por Instituto Nacional de Estándar Americano (ANSI) como software y hardware en su estándar

ANSI X3.92-1981. Posteriormente se sacó una versión de DES implementada por hardware, que entró a formar parte de los estándares de la ISO con el nombre de DEA.

DES, es un esquema de encriptación simétrico desarrollado por el Departamento de Comercio y la Oficina Nacional de Estándares de EEUU en colaboración con la empresa IBM, que se creó con objeto de proporcionar al público en general un algoritmo de cifrado normalizado para redes de computadoras. Estaba basado en la aplicación de todas las teorías criptográficas existentes hasta el momento, y fue sometido a las leyes de USA.

4.1.1.1.1.Caracteristicas del estándar .

(1) Una clave DEA consiste en 64 dígitos binarios de los cuáles 56 dígitos binarios sean generados y utilizados aleatoriamente directamente por el algoritmo. Los otros 8 dígitos binarios, que no son utilizados por el algoritmo, se pueden utilizar para la detección de errores. El error 8 que detecta dígitos binarios se fija para hacer la paridad de cada byte de 8 bits del impar dominante, es decir, hay un número impar de 1 en cada byte de 8 bits. Una clave de TDA consiste en 3 claves de DEA.

(2) DEA forma la base para TDA.

(3) Existen 4 diversos modos para usar DEA descrito en este estándar

- a. El modo Electrónico de Codebook (ECB), es una aplicación directa del algoritmo del DES para cifrar y para desencriptar los datos. Los bloques de texto se cifran por separado.
- b. El Encadenamiento de Bloque de cero (CBC), Los bloques del texto cifrado se relacionan entre sí mediante funciones *OR-EXCLUSIVA*.
- c. El modo de cifrado Feedback (CFB), Se realiza una *OR-EXCLUSIVA* entre caracteres o bits aislados del texto y las salidas del algoritmo. El algoritmo utiliza como entradas los textos cifrados.
- d. El modo Feedback de salida (OFB) Funciona igual que el CFB, pero utiliza como entradas sus propias salidas, por lo tanto no depende del texto; es un generador de números aleatorios.

4.1.1.1.2.Descripción del estándar.

El sistema parte de una clave de 64 bits, de los cuales se eliminan los 8 bits de paridad. Por lo tanto a todos los efectos se supone que la clave original K esta formada por 56 bits. La clave original K genera sucesivamente 16 claves $K_1, K_2, \ldots, K_{16}$ todas ellas de longitud 56.

El sistema cifra bloques de información M de 64 bits, en primer lugar aplica una permutación P fija y el bloque permutado se divide en dos subloques (L_0, R_0) cada uno de 32 bits. Posteriormente, para i = 1, . . . , 16 se aplica el proceso siguiente:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

al resultado final (L_{16},R_{16}) se le aplica la permutación P^{-1} y el resultado final es el cifrado del bloque M.

Generación de las subclaves:

La clave original de 64 bits se reduce a dos bloques de 28 bits, (C_0,D_0) convenientemente permutados por la permutación PC1. Cada uno formados por los bits (nótese que no se conserva su orden natural, si no que se permutan):

C_0=[57,49,33,25,17,9,1,58,50,42,34,26,18,10,2,59,43,35,27,19,11,3,60,52,44,36]
D_0=[63,55,47,39,31,23,15,7,62,54,46,38,30,22,14,6,61,53,45,37,29,21,13,5,28,20,12,4]

La clave Ki se forma entonces mediante:

$$C_i=LS(C_{i-1}),\ D_i=LS(D_{i-1})$$
$$K_i=PC2(C_i,D_i)$$

siendo:

- LS una permutación circular a la izquierda de una posición para i = 1, 2, 16 y de dos posiciones para los restantes índices.
- PC2 es una permutación junto con una selección de 48 de los 56 bits.

La función $f(R_{i-1}, K_i)$

La entrada de la misma son los 32 bits de R_{i-1} y los 48 bits de K_i. La función f viene dada por las siguientes operaciones:

- R_{i-1} se expande en $E(R_{i-1})$ que esta formado por 48 bits.
- B: E $E(R_{i-1}) \oplus K_i$
- $B=(B^1,\ldots,B^8)$ se reparte en 8 bloque de 6 bits cada uno.
- Se aplica B^i la función S_i, el resultado es $S_i(B^i)$ que está formado por 4 bits.

Las cajas Si, i = 1, . . . , 8 son una de las razones de la robustez del método. Cada una de ellas, S, es una tabla de doble entrada formada por 16 columnas (numeradas en binario 0000, 0001, . . .) y 4 filas (numeradas 00, 01, 10, 11). Cada fila de la tabla contiene una permutación de los enteros 0, 1, . . . , 15. Si el bloque de entrada es $b = (b_6b_5 \ldots b_1)$, la salida S(b) viene dada por la representación binaria del entero que corresponde a la fila b_6b_1 y la columna $b_5b_4b_3b_2$.

4.1.2. Criptografía asimétrica o de clave pública

Este sistema de cifrado permite que cada interlocutor tenga una pareja de claves propias. Una será la clave privada o secreta, y la otra la clave pública. La clave privada no se transmite nunca y se mantiene secreta. La clave pública, por el contrario, se puede y se debe poner a disposición de cualquiera dado que es imposible deducir la clave privada a partir de la pública.

La propiedad fundamental de esta pareja de claves es que lo que se cifra con una de ellas se descifra con la otra. La clave pública cifra los datos, pero no puede descifrar los mismos datos. Sólo la clave privada puede descifrar los datos que han sido cifrados con la clave pública.

En la siguiente figura se puede observar un ejemplo del funcionamiento de la criptografía asimétrica o de clave pública.

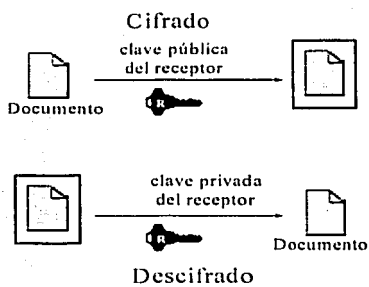


Figura 4.2 Algoritmo Simétrico de clave pública.

Con este sistema de cifrado de la transmisión se logra el primer requisito que se le exige a un sistema de comunicación seguro: la confidencialidad. Cualquier intruso que intercepte la transmisión no podrá descifrar el contenido de la misma al no poseer la clave privada del receptor.

Dentro de esta criptografía se encuentran los siguientes algoritmos de cifrado:

- **Sistema RSA:** Se basa en el hecho de que no existe una forma eficiente de factorizar números que sean productos de dos números primos muy grandes.
- **Sistema de Rabin:** Se basa también en la factorizacion.
- **Sistema de ElGamal:** Se basa en el problema del logaritmo discreto.
- **Sistema de Merkle-Hellman:** Esta basado en el problema de la mochila.
- **Sistema de McEliece:** Se basa en la teoría de la codificación algebraica.
- **Sistemas basados en curvas elípticas:** En 1985, la teoría de las curvas elípticas encontró de la mano de Miller aplicación en la criptografía. La razón fundamental que lo motivó fue que las curvas elípticas definidas sobre cuerpos finitos proporcionan grupos finitos abelianos, donde los cálculos se efectúan con la eficiencia que requiere un criptosistema, y donde el cálculo de logaritmos es aún más difícil que en los cuerpos finitos. Además, existe mayor facilidad para escoger una curva elíptica que para encontrar un cuerpo finito, lo que da una ventaja más frente a su predecesor, el sistema de ElGamal.
- **Sistema probabilístico:** Aunque la criptografía de clave pública resuelve el importante problema de la distribución de claves que se presenta en la criptografía de clave secreta; en clave pública se presenta otro problema, el texto cifrado C=Ek (M) siempre deja escapar alguna información sobre el texto original porque el criptoanalista puede calcular por sí mismo la función de cifrado con la clave pública sobre cualquier texto que quiera. Dado cualquier M' de su elección, puede fácilmente descubrir si el mensaje original M=M', pues esto se cumple si, y sólo si Ek(M')=C. Incluso aunque recuperar M a partir de C fuera efectivamente infactible, no sabemos cómo medir la información que deja escapar sobre M.

4.1.2.1. Algoritmo RSA (Rivest, Shamir, Adleman)

El algoritmo RSA fue descubierto por un grupo del M.I.T. y su nombre se deriva de las iniciales de sus autores: Rivest, Shamir y Adleman. La longitud de la llave es variable, la más

popular es de 512 bits, pero en la actualidad la llave de 1024 bits es comúnmente utilizada por el *Pretty Good Privacy* (PGP). [PGP 00], [YAMAMOTO 96] De igual forma el tamaño de bloques de datos RSA es variable, pero el bloque de texto plano (sin encriptar) debe ser menor que la longitud de la llave. El tamaño del texto cifrado es de la misma longitud que la llave.

El método seguido por el algoritmo es el siguiente:

Generación del par de llaves la pública y la privada.

1. Se eligen dos números primos muy grandes p y q (por ejemplo de 256 bits de longitud)
   Seleccionar p,q.
2. Hacer n = p * q y guardar en secreto p, q. Es prácticamente imposible obtener los factores de una n tan grande. Se llama modulo a n.
   n = p * q=modulo
3. Para generar la llave pública, se elige un número e, tal que $1 \leq e < \Phi(n)$, o sea menor a n que sea primo relativo a $\Phi(n) = (p-1)(q-1)$. Lo que significa que e y $\Phi(n)$ no tienen factores en común excepto al 1.
   $\Phi(n) = (p-1)(q-1)$
4. Sea la llave pública {e, n}. E es el exponente público.
   {e, n}
5. Para generar la llave privada, Calcular d que es el inverso multiplicativo (mediante el algoritmo de Euclídes extendido) de e mod Φ (n). De otra forma encontrar otro número d tal que (ed-1) sea divisible por (p-1)(q-1).
   $e\,d \equiv 1 \pmod{\Phi(n)}$
6. La llave privada es {d, n} D es el exponente privado. {d, n} Es necesario mantener secretos los números p, q y $\Phi(n)$

4.1.3. Firma Digital

Una firma digital es una cadena de datos creada a partir de un mensaje o parte de un mensaje de forma que sea imposible que quien envía el mensaje reniegue de él (***no repudio***) y quien recibe el mensaje pueda tener la certeza que quien dice que lo ha enviado es realmente quién lo ha enviado, es decir, el receptor de un mensaje con firma digital puede asegurar cual es el origen del mismo (***autenticación***). Así mismo, las firmas digitales pueden garantizar que el

contenido del mensaje no habrá podido sufrir modificación alguna durante su trayecto hasta el destinatario (***integridad***).

La firma digital se puede hacer sobre todo el mensaje que se envía o sobre un resumen del mismo. Esta segunda forma es mucho más eficiente.

Las funciones resumen (funciones HASH) son usadas para generar un resumen de los datos cuando se realizan firmas digitales. Estas funciones están basadas en el hecho que el resumen de un mensaje representa de forma concisa los datos originales desde los cuales va a ser generado. Debería considerarse como la huella digital de la más grande cadena de datos. Como las funciones de resumen son mucho más rápidas que las funciones de firma de todos los datos es mucho más eficiente utilizar la firma digital con un resumen que con todos los datos.

Los pasos necesarios para procesar una firma digital con funciones resumen serían los siguientes

el usuario prepara el mensaje a enviar.

- El usuario utiliza una función resumen segura para producir un resumen del mensaje.
- El remitente cifra el resumen con su clave privada. La clave privada es aplicada al texto del resumen usando un algoritmo matemático. La firma digital consiste en la encriptación del resumen.
- El remitente une su firma digital a los datos.
- El remitente envía electrónicamente la firma digital y el mensaje original (bien cifrado o bien sin encriptar) al destinatario.
- El destinatario usa la clave pública del remitente para verificar la firma digital (descifra el resumen enviado).
- El destinatario realiza un resumen del mensaje utilizando la misma función resumen segura.
- El destinatario compara los dos resúmenes. Si los dos son exactamente iguales el destinatario sabe que los datos no han sido alterados desde que fueron firmados (***integridad***), y que además el emisor sólo puede ser el poseedor de la clave privada que correspondiese a la clave pública con la que se descifró el resumen (***autenticación*** y ***no repudio***).

De este modo el receptor de los datos puede ahora asegurar que los datos transmitidos no han sido alterados.

Este esquema de funcionamiento se puede observar mejor en la siguiente figura. En ella se puede ver como el emisor genera un resumen, lo cifra con su clave privada y lo anexa al mensaje original. Por otro lado, el receptor recibe el mensaje y la firma, genera un resumen a través del mensaje con la misma función resumen conocida y además descifra con la clave pública del emisor la firma, comparando ambos resúmenes. Si tras esto se comprueba que son idénticos, la verificación de identidad e integridad es positiva.

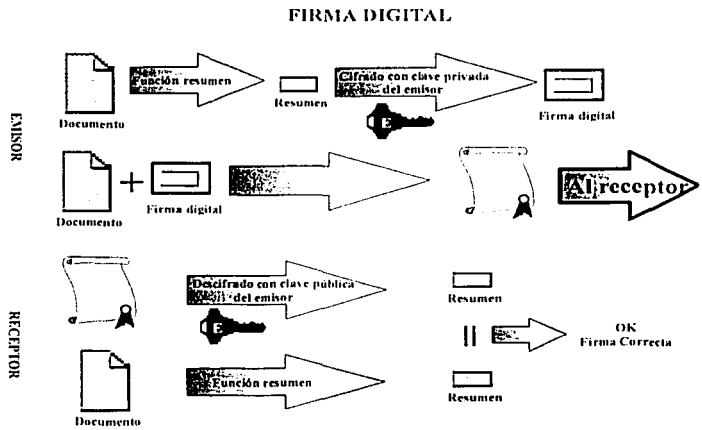


Figura 4.3 Diagrama de la Firma digital.

4.1.4. Técnica de "one way hash function"

En los procesos criptográficos se permite proteger la adquisición legal de la información, pero una vez obtenida la información se puede revender copias exactas.

Es así como una de las soluciones DRM para la comprobación de la autentificación de la manipulación digital es usando una técnica matemática llamada "*one-way hash function*". Una "*one-way hash function*" toma por ejemplo el contenido de texto con cualquier longitud

a modo de entrada y produce un pequeño mensaje de longitud fija, llamado "*message digest*". De esta forma un "*message digest*" es muy pequeño, digamos unos 128 bits, y ante cualquier cambio en el contenido que se toma a la entrada de la función "*one-way hash function*", producirá un mensaje totalmente diferente como resultado a la salida. O sea que si el contenido original fue procesado por el proveedor con la función "*one-way hash function*" y como resultado de esto dio un "message digest" como el siguiente:

"CABE88A801JJF1L8SDEKK8180MACD3B4"

El proveedor del contenido determina de esta forma que el sello de autenticidad de dicho contenido esta representado por este "*message digest*", como si fuese un sello estampado de autenticidad, que es guardado en forma segura y al que podría acceder el consumidor para determinar o verificar si el contenido que adquirió responde a dicho "*message digest*". Lo cual puede realizarse usando programas de amplia difusión para procesar "*message digest*" dentro ellos el llamando MD5 y verificar si al usar como fuente de entrada a dicho programa el contenido de texto que adquirió le da como resultado el establecido por el proveedor del contenido como sello de autenticación.

4.1.4.1. Algoritmo MD5

MD5, al igual que MD2 y MD4, fue desarrollado por Rivest en 1991, y es una versión mejorada de MD4.

El algoritmo MD5 realiza las siguientes operaciones:

1. Adición de bits de relleno:

El mensaje es rellenado o ampliado para que su longitud en bits sea congruente a 448 módulo 512. Esto debe ser así puesto que hay que reservar 64 bits para la adición de la longitud del mensaje en el próximo paso. Así pues, si no se llega a la anterior congruencia, se añadirá el relleno, consistente en un bit '1' seguido de tantos bits '0' como se precisen.

La razón de porqué un uno seguido de ceros se debe que si se emplea sólo relleno con un valor (por ejemplo todo ceros) el proceso no sería reversible a la hora de eliminar dicho relleno.

De todas maneras, siempre se realiza esta operación de relleno, aunque la longitud del mensaje ya sea congruente a 448 en módulo 512. Por ello, se añadirán como mínimo 1 bit de relleno, y como máximo 512 bits. Obsérvese la siguiente figura:

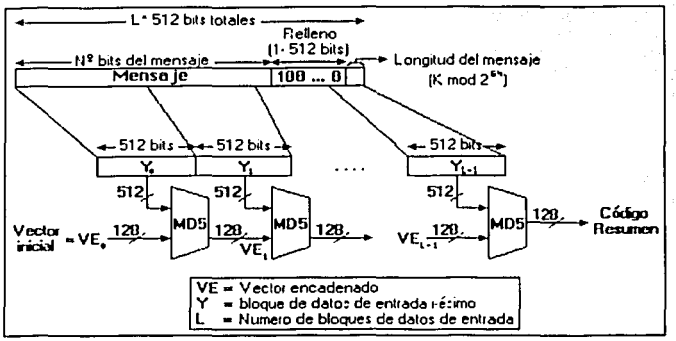


Figura 4.4 Operación de adición de bits de relleno.

2. Adición de representación binaria de longitud del mensaje:

Posteriormente se añade al mensaje (con el relleno realizado) una representación de la longitud del mensaje antes de ser rellenado. Dicha representación tendrá una longitud de 64 bits (16 palabras de 32 bits, es decir, dos enteros de 4 octetos cada uno). En el caso de que el mensaje sea mayor de 2^{64} bits, sólo se tendrán en cuenta los 64 bits menos representativos, que es lo mismo que decir que esta representación de la longitud del mensaje está realizada en módulo 2^{64}.

El mensaje tiene ahora un número de bits múltiplo de 512, por lo que habrá un número entero de palabras de 32 bits (enteros de 4 octetos), concretamente 512 / 32 = 16, de lo que se puede concluir que si hay b bloques de 512 bits cada uno que forman el mensaje, entonces el mensaje tendrá n palabras de 32 bits: n = 16 * b

3. Inicializar buffer MD:

Para poder calcular el valor hash o resumen se necesita tener un buffer de 4 palabras de 32 bits (A, B, C, D), pero antes de comenzar con el proceso se los ha de inicializar con algún valor determinado, que Rivest establece:

Palabra A = 01 23 45 67 67 45 23 01

Palabra B = 89 ab cd ef ef cd ab 89

Palabra C = fe dc ba 98 98 ba dc fe

Palabra D = 76 54 32 10 10 32 54 76

En la primera columna los valores hexadecimales están ordenados de modo que los valores menos significativos aparecen en primer lugar (notación empleada por Rivest en la implementación de este algoritmo), y en la segunda los valores más significativos están a la izquierda (posiciones más altas de la memoria en Intel 80xxx).

La razón de ver estas formas de representar los mismos valores se debe a intentar evitar confusiones, pues en función del tipo y arquitectura de la máquina sobre la que ha de trabajar el algoritmo, este sufrirá adaptaciones en dichos valores al realizar la implementación. Ello es debido a las distintas formas en que se almacenan los datos en memoria en las distintas arquitecturas (Intel, Sun, Spare, ...).

Los algoritmos MD4 y MD5 están pensados para facilitar su implementación en arquitecturas denominadas *little-endian*. Este formato asume que el byte menos significativo de una palabra se almacena en la posición más baja, y el byte más significativo en la parte más alta. Es el formato que emplean los procesadores Intel 80xxx que integran los PC domésticos.

En la primera columna se reflejan pues las constantes 'reales' que se emplean por el algoritmo, y en la segunda columna se encuentran los valores que se introducen para la inicialización en la versión codificada para arquitecturas
Intel 80xxx.

4. Procesar el mensaje en bloques de 512 bits:

Esta es la parte central del algoritmo. Se definen las cuatro funciones que se emplearán en las cuatro vueltas que se aplicarán sobre cada bloque. Ver la siguiente figura:

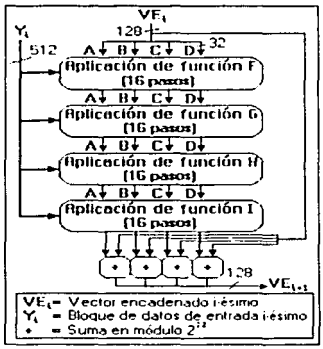


Figura 4.4 Diagrama de las funciones del algoritmo.

Estas cuatro funciones reciben como parámetros de entrada tres palabras de 32 bits cada una (tres enteros de 4 bytes de longitud) y devuelven como salida una. Son las siguientes:

F(X, Y, Z) = (X and Y) or ((not X) and Z)

G(X, Y, Z) = (X and Z) or (Y and (not Z))

H(X, Y, Z) = X Y Z

I(X, Y, Z) = Y (X or (not Z))

Donde F funciona como una sentencia condicional if en programación tradicional: Si X = 1 entonces Y será 1 de lo contrario Z será 1.

G también funciona de manera condicional como F: Si Z = 1 entonces X será 1 de lo contrario Y será 1.

H simplemente realiza la operación OR-Exclusiva (XOR) de X, Y y Z.

I realiza la operación XOR con X si es 1 o si Z es 0.

Para mayor claridad, obsérvese la siguiente tabla de verdad:

B	C	D	F	G	H	I
0	0	0	0	0	0	1
0	0	1	1	0	1	0
0	1	0	0	1	1	0
0	1	1	1	0	0	1
1	0	0	0	0	1	1
1	0	1	0	1	0	1
1	1	0	1	1	0	0
1	1	1	1	1	1	0

Figura 4.5 Tabla de verdad de las funciones.

Por otro lado MD5 no utiliza las constantes (*'magic' constants*) que se empleaban en MD4. En su lugar se emplea una tabla de 64 elementos construida a partir de la función trigonométrica seno. Sea T[i] el elemento i-ésimo de dicha tabla, que será igual a la parte entera de 4294967296 veces abs(sen(i)), donde i está expresada en radianes. Puesto que hay que realizar 16 pasos en cada una de las cuatro vueltas, es decir, 64 operaciones, la idea es usar una constante de la anterior tabla para cada vuelta. Los 64 valores son los siguientes:

1	3614060580	20	3921069994	39	4129429664	58	4264355552
2	3905402710	21	3593408605	40	3290256656	59	2734768916
3	606105819	22	38016083	41	681279174	60	1309151649
4	3225406846	23	3634488961	42	3956430074	61	4149444226
5	4118548399	24	3889429448	43	3572445317	62	3174756917
6	1200080426	25	568446438	44	760029189	63	718787259
7	2821735955	26	3275163606	45	3654602809	64	3951481745
8	4249261313	27	4107603335	46	3873151461		
9	1770035416	28	1163531501	47	530743520		
10	2336552879	29	2850285829	48	3299628645		
11	4294925233	30	4243563512	49	4096336452		
12	2304263134	31	1735328473	50	1126891415		
13	1804606682	32	2568359562	51	2878612391		
14	4254626195	33	4294588738	52	4237533241		
15	2792965006	34	2272392833	53	1700485571		
16	1256535309	35	1839045962	54	2399980690		
17	4129170786	36	4259657740	55	4293915773		
18	3225465664	37	2763975236	56	2240044497		
19	643717713	38	1272893353	57	1873313359		

Figura 4.6 Tabla elementos T[i]=4294967296 abs(sen(i)), i=1,...,64

Para mayor claridad a la hora de comprender la construcción de función en cada uno de los 64 pasos (por bloque), véase la siguiente figura:

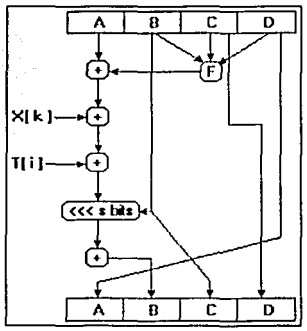


Figura 4.7 Diagrama de construcción de función.

5. Recoger el valor hash de salida:

El valor hash de salida se obtiene de los registros A, B, C y D donde el octeto más representativo es D y el que menos A.

Por último, a modo de ejemplo se presentan una serie de entradas e para ver sus correspondientes salidas s tras la aplicación de este algoritmo:

e:""

s: d41d8cd98f00b204e9800998ecf8427e

e: "a"

s: 0cc175b9c0f1b6a831c399e269772661

e: "abc"

s: 900150983cd24fb0d6963f7d28e17f72

e: "message digest"

s:f96b697d7cb7938d525a2f31aaf161d0

e: "abcdefghijklmnopqrstuvwxyz"

s: c3fcd3d76192e4007dfb496cca67e113b

e: "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"
s: d174ab98d277d9f5a5611c2c9f419d9f

e:
"12345678901234567890123456789012345678901234567890123456789012345678901234
5678
s: 57edf4a22be3c955ac49da2e2107b67a

4.2. Técnica de Marcas de Agua (Watermark)

Una watermark o marca de agua digital, algunas veces llamada "huella digital", permite a dueños con derechos de autor incorporar identificación en su trabajo; información invisible al ojo humano.

Las técnicas de Marca de Agua son utilizadas para la autenticación (tanto del distribuidor o propietario legal, como de que el original no ha sido falsificado) de la información, así como para el seguimiento de copias, ya que permiten la identificación del autor, propietario distribuidor y/o consumidor autorizado de un contenido digital.

Pueden complementar a la codificación insertando una señal secreta e imperceptible, una "marca al agua", directamente sobre los datos originales de tal forma que permanezca siempre presente. La Marca de Agua consiste en sumar a la imagen original otra imagen de amplitud muy pequeña, de tal forma que no sea perceptible.

La Marca de Agua es una técnica esteganográfica

4.2.1. Requisitos de Marca de Agua

Diferente a la encriptación la cual es "útil para la transmisión", pero no proporciona una forma para examinar el dato original en su forma protegida, la marca de agua, permanece en el contenido en su forma original y no facilita al usuario de escuchar, ver, examinar, o manipular el contenido.

Dependiendo del tipo de aplicaciones podrán utilizarse los diferentes requisitos que a continuación se describen.

- **Transparencia perceptible:** aunque si se comparan los datos originales con los marcados se puede apreciar cualquier diferencia introducida, los usuarios no van a tener acceso a esos datos originales, así que no podrán realizar esta comparación.
  Entonces se dice que una marca es realmente imperceptible si no se pueden distinguir los datos originales de los marcados, teniendo en cuenta que no se pueden comparar directamente, la calidad de una imagen con marca de agua debe ser muy alta, en general Pick Signal to Noise Ratio (PSNR) mayor o igual a 30 dB, significa que la calidad de la imagen modificada sea aceptable. La marca de agua embebida debe ser recuperable sin usar información de la imagen original, en otras palabras, no será permitido almacenar una copia de la imagen.
- **Carga útil de la marca:** es la cantidad de información que puede ser almacenada en una marca. Un concepto importante relacionado con la carga útil es la granularidad de la marca que representa cuántos datos son necesarios para insertar una unidad de información de la marca. Por ejemplo, para vídeos digitales la más pequeña entidad que puede protegerse con derechos de autor es un fragmento de un segundo

(aproximadamente 25 *frames* o marcos de imagen). Entonces, la marca deberá insertarse en menos de un segundo de vídeo. Si esta marca consta de 70 bits, tendríamos un canal de información de 70 bps.

- **Robustez:** dependiendo de la aplicación será más o menos conveniente que la marca sea robusta. Por ejemplo, si queremos detectar si los datos han sufrido la más mínima alteración, querremos una marca débil que se vea degradada fácilmente. Así, al recuperar la marca y comprobar que no es igual a la original, sabremos que los datos que la contenían han sido manipulados. Para otras aplicaciones, sin embargo, se quieren marcas que no desaparezcan aun cuando los datos hayan sido seriamente deteriorados. Por ejemplo, ante una compresión con pérdidas o un filtrado.
- **Seguridad:** una técnica de marca de agua es realmente segura cuando el conocimiento de los algoritmos de inserción/extracción de marcas no es suficiente para eliminarlas. Se necesita conocer una clave.

El uso de marcas de agua como método para proteger la propiedad intelectual es relativamente reciente, pero se basa en conceptos ampliamente utilizados en otros campos: como comunicaciones de espectro expandido y teoría de ruido.

Similar a la criptografía la seguridad en las marcas de agua no puede ser basada en la suposición de posibles atacantes, de que no sepan como la marca fue embebida en la imagen. Aun cuando el atacante sepa como la marca de agua fue embebida solo el dueño de los derechos de autor, debe saber como detectar o como remover su marca de agua de su imagen. Debe ser posible extraer la marca de agua después de múltiple y varios procesamientos en la imagen, así como filtrado de paso bajas o filtración de paso altas, compresión con perdidas, adaptación a escala, etc, previendo que la calidad de la imagen alterada sea aceptable

Para insertar una marca en los datos existen muchas técnicas. Estas técnicas consisten en realizar pequeñas modificaciones en los datos, de tal forma que sean visualmente imperceptibles. Es en estas modificaciones donde reside la información de la marca.

Se pueden realizar muchas modificaciones para insertar una marca, en el dominio del tiempo (o del espacio, en el caso de las imágenes), y en el de la frecuencia. Por ejemplo, se pueden modificar los bits menos significativos de la información, sumar un ruido, eliminar o reordenar algunos coeficientes de la transformada de los datos, deformar parte de los datos, imponer semejanzas entre bloques, etc.

4.2.2. Técnicas basadas en procesamiento en el dominio del espacio

Los primeros trabajos propuestos para realizar el proceso de marcado en el dominio del espacio se basaban en la modificación del Bit Menos Significativo Less Significant Bit, (LSB) de los pixeles localizados en áreas seleccionadas por secuencias de números pseudo-aleatorias. Estos métodos son muy sencillos de implementar y producen algoritmos muy rápidos, pero cualquier pequeña variación producida por filtros o compresiones altera casi siempre estos bits y por consiguiente elimina la marca. Tiene dos desventajas: baja seguridad y genera una marca muy robusta.

4.2.2.1. Método del automorfismo toroidal (*Torus automorphism*) para la inserción de marcas de agua digitales.

Un automorfismo toroidal es un sistema dinámico. Brevemente, un sistema dinámico es uno cuyo estado s cambia con el tiempo t. Cuando t es discreta, un sistema dinámico puede estar representado como:

$$s_{t+1} = f(s) \quad t \in Z$$

t que es una iteración de una función f.

Un automorfismo toroidal bidimensional es representado aquí. Puede considerarse como una transformación espacial de una región de un plano. Esta transformación se desempeña usando una matriz A de 2 x 2 con todos sus elementos constantes. Un estado o punto s' = (x',y') que se obtiene de la ecuación (3) usando el punto s =(x,y)

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod 1 \quad \ldots.(3)$$

Donde $|A|$ denota el determinante de A. En (3), $a_{ij} \in Z$ $|A|=1$, y A tiene valores propios es $\lambda_{1,2} \in R$ {-1,0,1}. Un conjunto de puntos $\{s_0, s_1, s_2, \ldots\}$ es una órbita O del sistema. El punto inicial $s_0=(x_0,y_0)$ clasifica O dentro de dos categorías. Cuando x_0 y y_0 con racionales, O es periódica cada R tiempo ($s_R = s_0$). R es llamado "tiempo de recurrencia". Si x_0 y/o y_0 son irracionales, O es infinita.

Analizaremos primer caso cuando el primer punto siempre es racional.

Un primer-parámetro del automorfismo toroidal se introduce como se indica a continuación. Este sistema se aplica en el esquema :

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \bmod N \ldots (4)$$

donde $(x_i, y_i) \in [0, N-1] \times [0, N-1]$ y $k \in [1, N-1]$. El tiempo de reaparición R depende de los parámetros k y N y del punto inicial (x_0,y_0). Se concluye que en la mayoría de los casos R es igual a N - 1 o N + 1 cuando N es primo. Hay otras condiciones que hacen irregular a R. El sistema en (4) se usa para proveer la información de ubicación a través de A. La información de ubicación consiste que aproximadamente los elementos de la marca de agua se combinen con la imagen *host*. Nótese que un generador pseudo - aleatorio de números puede utilizarse para proveer la información de ubicación, pero el método del automorfismo toroidal provee una manera más conveniente para implementar este esquema.

La idea principal de proponer un esquema es para determinar una regla de mapeo para pasar de los elementos de la marca de agua a los elementos de la imagen original. Esta regla se registra como una matriz P, llamada llave secreta, que tiene las mismas dimensiones que la marca de agua. La matriz registrada P se usa luego para calcular la marca de agua. Además, la P será firmada como Ps, mediante terceras partes confiables y será la evidencia que se usará para identificar el verdadero propietario intelectual del derecho de propiedad (IPR).

Tanto la imagen original O como la marca de agua W requieren β bits por píxel. En este ejemplo se usa un β igual a 8. O y W son definidas como siguen:

$O = o_{i,j}, i = 1,2,\ldots,O_H, j = 1,2,\ldots,O_w$

$$0 \le o_{i,j} \le 2^{\beta} - 1 \quad (5)$$

$W = w_{i,j}, i = 1,2,\ldots,W_H, j = 1,2,\ldots,W_W$

$$0 \le w_{i,j} \le 2^{\beta} - 1 \quad (6)$$

Aquí O_H y O_w son la altura y anchura de la imagen original respectivamente. W_H es la altura de la marca de agua y W_w es la anchura de la marca de agua. Los parámetros del sistema del automorfismo toroidal son k y N. El criterio para elegir k y N crea el tiempo de reaparición $R \ge 2^{\tau}$, pero no es esencial. Aquí τ es la longitud de los elementos de P. La matriz A^t es definida como sigue:

$$A^t = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix}^t \bmod N \quad (7)$$

$P=\{p_{i,j} \quad i=1,2,...,W_H, j=1,2,...,W_W \}$ esta construido por:

$p_{i,j}=t$. tal que $O_{i'_{t,j}} - w_{i,j} = \min_{0\le t<2^r}\left(O_{i'_{t,j}} - w_{i,j} \right)$ (8)

donde $0<t<2^r$; i= 1, 2,..., W_H, j= 1,2,..., W_W y $O_{i'_{t,j}} = o_{i',j'}$ (9)

$(i', j')=(i, j)x\ A^t \bmod (O_H, O_W)$ (10)

Brevemente $O_{i'_{t,j}}$ es un valor del pixel de la imagen original en las coordenadas (i', j'). Aquí (i', j') es determinado por A, t, y (i, j). Después que P sea generada, el proceso de generación de la llave se completa. Claramente, la imagen protegida es la misma que la imagen original en el esquema propuesto. En otras palabras, La imagen original nunca se modifica aun cuando se proteja. El dueño de la imagen envía P a Terceras Partes para obtener *time stamping* P como Ps. Ps es usada como evidencia que la llave secreta P sea generada de una imagen O en un cierto tiempo. El dueño tiene que guardar k, N y Ps secreta.
La marca de agua de la imagen del propietario W puede ser calculada por:

$$w'_{i,j} = O^{p_{i,j}}_{i'_{t,j}}, i=1,2,...,W_H, j=1,2,...,W_W \quad (11)$$

Cabe mencionar que la marca de agua computada W es diferente de la original marca de agua W. la distorsión es ocasionado por (8). Sin embargo la distorsión es aceptable.

4.2.3. Técnicas basadas en procesamiento en el dominio de la frecuencia

Los métodos basados en el procesamiento en el dominio de la frecuencia calculan una transformada en frecuencia de la imagen, seleccionan algunos de los coeficientes que definen la imagen en el dominio transformado, modifican los valores de algunos de ellos y vuelven a calcular la transformada inversa. Embebe la marca de agua después de usar la transformada de Fourier, Coseno Discreto o Wavelet. La diferencia fundamental entre estos métodos es la función que define la selección de los coeficientes a modificar y la cantidad de dicha modificación.
Para la extracción de la marca, en primer lugar hay que seleccionar las posiciones donde se encuentra (tanto si se marca en el dominio de la frecuencia como en el del espacio). Este proceso suele requerir el original o la marca añadida para realizar la comparación. También es posible extraer la marca sin el original, para lo cual el algoritmo debe detectar propiedades específicas y patrones del documento marcado.

Si hay una jerarquía en la inserción de marcas (inserción de varios códigos de identificación y extracción por separado), debe cuidarse el orden de inserción pues la inserción de una marca sobre una imagen ya marcada puede dañar tanto la imagen como la marca (creará ruido adicional que puede degradar la información hasta hacerla irrecuperable). Por otra parte la aparición de varias marcas sobre la misma imagen puede crear problemas a la hora de determinar la autoría de la misma.

Capítulo 5

DRM- Rich y DRM-Lite.

5. DRM- Rich y DRM-Lite

La tecnología DRM puede ser separada en dos componentes:

(a) DRM-*Rich* (DRM-R)

(b) DRM - LITE

Cada componente agrega funcionalidad y complejidad, según la naturaleza del contenido que debe ser protegido.

Los perfiles de DRM-*Rich* define una solución de DRM completa posibilitando una extensión de una red fiable, que incluye dispositivos abiertos de OS como ejemplo PCs a través de cifrado. Esta solución es intrínsicamente más compleja, permite la separación de Administración de Contenidos y Derechos asociados a través de diferentes accesos a redes como Internet.

Este tipo de soluciones es considerado más apropiado para la distribución de contenidos de valor alto como pueden ser libros electrónicos (e-Books), CD y DVDs ver la Figura 5.1. Aunque veremos más tarde de que con los tipos de sistemas criptográficos anteriormente estudiados podemos autenticar al comprador, y garantizar que el material ha sido entregado a la persona esperada sin que nadie haya podido realizar copias ilícitas durante la transmisión.

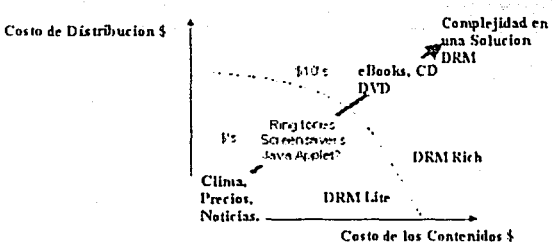


Figura 5.1 Gráfica que explica la complejidad de un Sistema DRM, en función del costo de los contenidos y de su distribución.

¿Por qué tenemos una necesidad de DRM-lite?

Los fenómenos siguientes conducen a la necesidad de DRM móvil:

- El surgimiento de formatos de multimedia-móvil llamados de *new media*: el teléfono móvil se ve como un camino nuevo de consumir contenido digital, hasta en sus formas más ricas y capacidades: Además de la llegada de Mensajería multimedia, también se explotan formatos nuevos de contenidos que son tonos de timbrado, salvapantallas, aplicaciones Java, etc. Los cuales comparte la exigencia inmediata de protección de transmisión y su posterior re-transmisión.
- La optimización móvil: La solución de DRM basada en PC no es directamente aplicable a un entorno móvil (reduciendo la amplitud del ancho de banda, el tiempo de conexión, etc.) Además, ellos no utilizan las oportunidades intrínsecas (como la autenticación fácil para el pago) del canal móvil.
- "La lección Napster". Proveedores de contenidos que han aprendido que la combinación de contenidos sin protección y lo que un enorme volumen puede hacer. Esta vez, ellos exigirán la protección para liberar el contenido.
- El éxito del sistema de negocio de tonos de timbrado/ logos: Siendo ya un negocio de multimillones de dólares en el mundo Short Messages Service (SMS), los SMS de *ringing tones* (tonos de timbrado) ha demostrado un exitoso *win-win* todos ganan para el proveedor del modelo de negocio
- La Facilidad en la facturación por parte del distribuidor en este caso el operador móvil: la facturación del operador es sobre todo conveniente para el valor bajo, impulsando la compra de multimedia.

El perfil de contenidos para DRM - LITE es implementado para redes confiables, caracterizado por dispositivos móviles OS móviles, donde el consumo es implementado por las políticas de la empresa y no incluye forma alguna de cifrado.

DRM - LITE permite a los proveedores de contenidos definir reglas de consumo, como por ejemplo:

- adelantar, salvar o guardar y la vista previa.

DRM - LITE puede ser considerado apropiado para contenidos de valores bajos, grandes volúmenes de contenido que son entregados dentro de M-Services y Tercera Generación.

Como ejemplo de los contenidos de valores bajos se encuentran:

Noticias, tiempo y precios.

Informes privilegiados como recomendaciones de analistas para la compra/venta
Tonos de timbrado, salvapantallas y aplicaciones Java.
Por esto los creadores de contenidos, dueños de contenidos, operadoras móviles y fabricantes de móviles están sumamente interesados en la implementación de esta nueva tecnología.

5.1. Administración de derechos digitales de contenidos transmitidos por una red móvil.

5.1.1. Alcance

Debido a las capacidades limitadas del equipo de usuario y costo de los contenidos, este apartado se dirige esencialmente para la tecnología de DRM - LITE para redes-originales adaptadas a multimedia de entretenimiento dentro de una estructura de entrega de M-Services.

- **Media Object:** son objetos descargables como salvapantallas, tonos de timbrado.
- **Rights Information File:** el Archivo que describe reglas de uso asociadas con un *media object*.
- **UE:** Equipo de Usuario, típicamente un handset móvil.
- **Removable Memory Device:** periférico de memoria que puede ser removido del UE.
- **DRM User Agent:** una aplicación residente en un UE, que implementa las reglas especificadas en los archivos de información de derechos.

5.1.2. Arquitectura DRM-Lite

Al hablar de la arquitectura empezaremos definiendo una red fiable.

5.1.2.1. Definición de una red Fiable

Una red fiable, tiene las siguientes características:

- El contenido es transferido entre el autor, dueño o creador del contenido y la red fiable (ver figura 5.2) sobre redes seguras intermedias protegidas por ejemplo con Secure Sockets Layer (SSL), Transport Layer Security (TLS) o Internet Protocol Security (IPSec).
- La entrega de contenidos dentro de una red fiable es segura usando Wireless Transport Layer Security (WTLS).
- Los contenidos recibidos, los elementos constituyentes (del UE) dentro de una red fiable deberán cumplir la distribución y reglas de consumo apropiadas.

- Una vez entregado el contenido en una red fiable, este no puede ser transferido fuera de dicha red.
- La arquitectura de sistema DRM proporciona la capacidad de restringir la transmisión (descarga) de medios/contenidos protegidos en una UE fiable. Una posible implementación o puesta en práctica es preguntar o interrogar al Perfil de Agente de Usuario del dispositivo para verificar si soporta la Administración de Derechos.

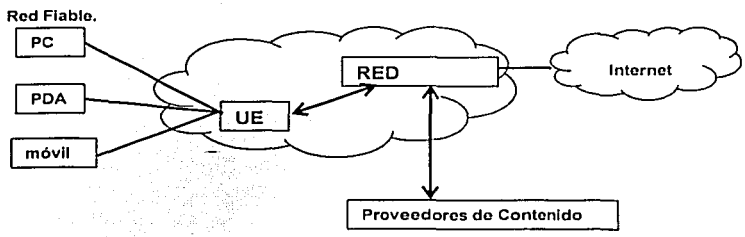


Figura 5.2 Definición de una red fiable.

5.1.3. Implementación de condiciones Fiables.

La arquitectura DRM controlará la distribución de objetos de multimedia implementando los derechos. Debido a las múltiples opciones de conectividad, la implementación de derechos es requerida sobre ambos UE vía un Agente de Usuario DRM y dentro de la red para prevenir la distribución no autorizada. La siguiente tabla resume los diferentes escenarios de distribución.

5.1.4. Escenarios de Distribución.

Mecanismos	Escenarios de Distribución
Mensajería 1	Usan re-envíos "*forwards*" de objetos mediante el cliente de mensajería
Mensajería 2	Usuarios establecen re-envíos "*forwards*" en cuentas de e-mail de Internet en centros de servicio de mensajería o servidores
Dispositivo de Memoria Removible	El usuario distribuye un objeto mediante el dispositivo de memoria removible
Conectividad Local (Bluetooth/IrDA, USB etc.)	El usuario transfiere un objeto vía Bluetooth, IrDA, USB, etc.

1. **Conectividad Local.** El UA de DRM previene la distribución hacia adelante vía la conectividad local por Ejemplo: Bluetooth, Universal Serial Bus (USB), Infrared Data Association (IrDA) etc.
2. **Memoria Removible.** El UA de DRM administra los derechos de cifrado que permiten a los objetos de multimedia ser almacenados en los dispositivos de memoria removible según las reglas especificadas.
3. **Re-Envío de Mensaje a UE No-compatible.** El re-envío del mensaje a las entidades fiables es restringida por la red (por ejemplo la interrogación de User Agent Profile (UAProf))
4. **El re-envío de Mensaje y Desvíos a Internet.** Los mensajes que contienen objetos manipulados por derechos no son re-enviados, por el UE, o desviados, por la red (por ejemplo esto se implementaría usando un Proxy/cortafuego).

Nota: estas medidas apoyan la distribución dentro de un dominio de una red fiable. Los dominios pueden comprender los grupos de redes móviles, comprometido según acuerdos del nivel de servicio, y permite la distribución inter- Public Land Mobile Network (PLMN) de contenido en origen por la red. La arquitectura de User Equipment (UE) DRM.

La arquitectura de sistema del UE DRM consiste de las entidades siguientes:

- **Agente de Usuario DRM:** El Agente del Usuario de DRM (UA) maneja objetos de multimedia y la información de derechos asociada y es el responsable de implementar las reglas especificadas dentro del archivo de información de derechos. Los clientes UE son responsables de iniciar el DRM UA cuando el objeto de multimedia protegido es detectado.
- **Cliente de MMS:** Es un cliente de Servicio de Mensajería Multimedia (MMS) Para el usuario del teléfono, MMS es muy similar al Servicio de Mensajes Cortos (SMS): permite el envío automático e inmediato de contenidos creados por el usuario de un teléfono a otro, los mensajes MMS pueden incluir imágenes estáticas, voz o secuencias de audio, y próximamente también vídeos e información en forma de presentaciones. Un mensaje MMS es una presentación multimedia en una sola entidad, y no un archivo de texto con datos adjuntos.
- **SMS/EMS:** Short Message System SMS es una característica del estándar GSM que permite enviar mensajes de texto de hasta 160 caracteres en redes GSM a teléfonos móviles o enviar mensajes entre teléfonos móviles Enhanced Messaging Service (EMS) los usuarios móviles pueden dar vida a sus mensajes cortos incluyendo melodías, imágenes y animaciones
- **Browser o Visualizador:** Es el programa que permite explorar textos, videos, gráficos, sonido y fotos en Internet.
- **Java Runtime Environment:** JRE es la Plataforma Java estándar mínima para ejecutar programas Java. Contiene la Máquina Virtual Java (MVJ), las clases centrales de Java y los archivos de soporte
- **Media Player**: Software que será capaz de reproducir archivos de Media.

5.1.5. Requisitos técnicos para DRM-LITE.

Esta sección define las exigencias de conformidad generales de política y de aplicación para DRM - LITE.

5.1.5.1. Agente de Usuario y política

(1) Cualquier objeto de multimedia del Agente de Usuario de DRM implementa las reglas especificadas en el archivo de información de derechos asociado (RIF).

(2) El Agente de Usuario DRM provee 'seguridad de almacenaje' del objeto de multimedia y derechos asociados. Éste incluye el medio para asociar los derechos con un objeto de multimedia.

(3) Los derechos a los que no serán accesibles, son:

a) No será posible corregir (editar) los derechos usando el UI.

b) No será posible suprimir (borrar) los derechos usando el UI.

c) No será posible sobrescribir los derechos usando el UI.

(4) El Agente de Usuario DRM proporciona la habilidad de asegurar, por medio del encriptado, el almacenamiento de objeto de multimedia en dispositivos de memoria removible tal que los objetos archivados o almacenados no pueden ser leídos por otros dispositivos (por ejemplo: una computadora personal u otro UE)

(5) El Agente de Usuario DRM impide el manejo de los derechos de los objetos multimedia para que sean exportados desde el UE vía conexiones locales, por ejemplo: USB, Bluetooth o IrDA.

(6) Cuando el contenido es suprimido (borrado) los derechos asociados son suprimidos (borrados) con cualesquier referencia.

5.1.5.2. Manejo de Derechos en la Estructura del Contenido

(7) La presencia de objetos protegidos por derechos son indicados dentro del HTTP multipart/relacionado o Wireless Session Protocol (WSP) vnd.wap.multipart.mixed cabecera MIME, ilustrados en la figura de abajo.

```
Content-Type = multipart/related; boundary = object-boundary
Start = ''<rights_information_file>''
--object-boundary
Content-type: xml/RIF
Content-ID: <rights_information_file>
Content-Description: document describing the consumption rules for the
associated media object
[RIF file here]
--object-boundary
Content-type: image/jpeg
Content-ID: <image_object>
Content-Description: protected object
[image object here]
--object-boundary
```

Estructura MIME Multipart/related para la protección de los contenidos.

(8) El manejo de derechos en la estructura de contenidos será representado por el siguiente conjunto de características:

US-ascii (IANA MIBEnum 3)

Utf-8 (IANA MIBenum 100)

Utf-16 (IANA MIBenum 1000)

(9) El manejo derechos en la estructura de contenidos debería usar extensiones WAP Binary eXtended Markup Language (WBXML) para mejorar la eficacia de transmisión.

Nota: Los elementos WBXML puede ser esenciales donde los objetos son entregados vía Connectionless WSP PUSH que usa SMS como el acceso a una red. El conjunto de código de WBXML es específico para los derechos en un lenguaje definido y está por definirse.

5.1.5.3. Conformidad de Browser

(10) Donde la estructura multipart/related (o el equivalente) es indicada, el objeto RIF es indicado por el parámetro start.

5.1.5.4. Conformidad de MMS

(11) Dentro del contexto de MMS, el manejo de la estructura de los derechos esta definida dentro del cuerpo del mensaje.

(12) Incluyendo un componente de Administración de derechos en la arquitectura de entrega de MMS, y adoptando las mismas simplificaciones de conformidad para reducir al mínimo la complejidad, el cuerpo de mensaje será flexible, de conformidad con el archivo RIF como el segundo objeto en la estructura de MIME

La modificación del manejo de derechos en la estructura MMS se ilustra a continuación:

```
Content-Type = application/vnd.wap.multipart.related; boundary = object-boundary
Start = <MMS_SMIL>
  -object-boundary
Content-type: application/SMIL
Content-ID: <MMS_SMIL>
Content-Description: MMS SMIL presentation
  -object-boundary
Content-type: xml/RIF
Content-ID: <rights_information_file>
Content-Description: document describing the consumption rules for the associated media
object
[RIF file here]
  -object-boundary
Content-type: image/jpeg
Content-ID: <MMS_image>
Content-Description: MMS protected image object
[image object here]
  -object-boundary
Content-type: text/plain
Content-ID: <MMS_text>
Content-Description: MMS text
  -object-boundary
```

Estructura de MMS que tiene asociado unos derechos de uso.

5.1.6. Definición del Lenguaje Rights Information File RFI

(13) El lenguaje para la definición de derechos será Open Digital Rights Language (ODRL)

(14) Específicamente, la RIF basada en ODRL soportará:

a) Una versión de referencia.

b) ***UID***. La referencia única para el objeto manejado. El UID será definido por el URI (Uniform Resource Identifiers) o el MIME Content-ID.

c) ***Display***. Este atributo permite la interpretación de un objeto gráfico dentro de la pantalla del UE.

d) ***Play***. Este atributo permite la interpretación de objetos de audio y de vídeo.

e) ***Execute***. Este atributo permite a un objeto ser dado en la forma legible por la máquina (por ejemplo una aplicación Java)

f) **Uso de restricciones.** ***Display, play y execute***: Un valor de 0 no significara el límite del número de veces en que un objeto puede ser dibujado o creado.

g) ***Copy***: Este atributo permite la extracción de uno o más objetos de la estructura MIME y define su reutilización.

h) ***Reuse-Copy-Constraints-User***: **Individual**. Este atributo define el número de copias que se permiten.

i) ***Reuse-Copy-Constraints-Device: Storage***: Este atributo define el número de las copias que pueden ser conservadas sobre el UE. Un valor de 0 almacenaje principal no es posible.

j) ***Narrow***. Este atributo permite al UE modificar los derechos del down-stream para objetos copiados.

k) ***Modify***. Este atributo permite al UE controlar la modificación de los objetos.

l) ***Give***. Este atributo permite la transferencia de objetos y derechos asociados a otro UE dentro de una red fiable. Es asumido que este proceso implicaría un método de reconocimiento que asegura que una vez que el objeto y los derechos asociados son transferidos a otro UE el objeto original y derechos son borrados del UE remitente.

(15) Donde las derechos de los objetos tienen una expiración, al usuario se le presentan dos opciones:

- Actualizar la licencia y re-direccionar al usuario al servidor de contenido apropiado.

- Actualizar la licencia y re-direccionar al usuario al servidor de contenido apropiado.
- Borrado del objeto junto con los derechos asociados y referencias.

5.1.7. Método de Ataque

En la ausencia de cifrado la arquitectura descrita anteriormente es objeto de ataque, y el método más obvio se presenta cuando una PC esta conectada a una Red a través de una tarjeta de datos. En este escenario la PC con una pila de protocolo WAP y parámetros modificados puede simular un legítimo móvil con cliente MMS o un cliente visualizador para recibir contenido. Dentro de un ambiente de PC el RFI puede ser modificado y como consecuencia duplicarse el objeto multimedia asociado sobre Internet sin ninguna restricción.

5.1.8. Definiciones utilizadas en el capítulo.

- **Bluetooth:** Bluetooth™: Una iniciativa global de Ericsson, IBM, Intel, Nokia y Toshiba para fijar un estándar para la conectividad inalámbrica entre teléfonos móviles, las PC móviles y otros dispositivos.
- **IrDA:** La asociación de datos por infrarrojos (Infrared Data Association, IrDA) es una organización patrocinada por la industria y establecida en 1993 para crear estándares internacionales para el equipo y programas usados en los enlaces de comunicación por infrarrojos. IrDA-Data, permite la comunicación bidireccional entre dos extremos a velocidades que oscilan entre los 9.600 bps y los 4 Mbps. Esta oscilación depende del tipo de transmisión (síncrona o asíncrona), la calidad del controlador que maneja los puertos infrarrojos, el tipo de dispositivo, y por supuesto, la distancia que separa ambos extremos. Precisamente, éste es uno de los puntos más problemáticos, ya que aunque la distancia entre emisor y receptor puede alcanzar los 2 metros, no se recomienda superar uno. Por no hablar de los puertos de bajo consumo instalados en móviles y pequeños PDAs, cuyo rango de acción se reduce a no más de 30 cm. En cualquier caso, hemos de situar los artículos en un ángulo máximo de 30 grados y contar con un espacio libre de obstáculos entre ellos.
- **HTTP:** es la abreviatura de Hypertext Transfer Protocol (Protocolo de Transferencia por Hipertexto). Es un conjunto de reglas, o protocolo, que gobierna la transferencia de hipertexto entre dos o más computadoras. La World Wide Web agrupa el universo de información que está disponible via HTTP. Hipertexto es texto codificado

especialmente usando un sistema estandar llamado Hypertext Markup Language (Lenguaje de Marcado por Hipertexto) (HTML).

- **MIME:** Multipurpose Internet Mail Extension, o extensiones multiuso para el correo en Internet MIME es un protocolo que permite pegar o adjuntar los archivos o binarios, como los jpeg, gif, etc. a los mensajes de e-mail. Si los destinatarios disponen del mail reader (lectores de correo) que utilizan el protocolo MIME, podrán extraer y utilizar los archivos que se les han enviado. Por ejemplo, MIME puede ser utilizado para insertar en un mensaje de e-mail un documento en Microsoft Word para Windows. Si el lector de correos del destinatario utiliza el protocolo MIME, éste podrá extraer el documento Word del mensaje de e-mail.
- **M-Services:** The Mobile Services Initiative (M-Services) aspira a consolidarse como un estándar abierto de software, en donde los principales fabricantes y operadores del sector de la telefonía móvil han puesto en marcha una iniciativa mundial para hacer del acceso a Internet móvil una realidad, en términos de alcance y utilidad. M-Services aportarán consistencia en áreas como el diseño gráfico, música, vídeo y juegos sobre GPRS.
- **PLMN:** Es una red establecida y gestionada por una agencia reconocida para el propósito específico de prestar servicios terrestres móviles al público. Un PLMN se puede considerar como una extensión de una red fija como una red pública conmutada (PSTN).
- **Streaming:** puede traducirse como "flujo de datos", o simplemente como flujo; es una tecnología que les permite a los usuarios apreciar, casi en tiempo real, secuencias de multimedia desde Internet aun disponiendo de conexiones tan lentas como 28,8 Kbps, esto es posible gracias a que una secuencia se puede reproducir antes que la totalidad del archivo que la contiene haya bajado al disco. Se habla de multimedia porque streaming no solo permite apreciar audio y video; también presentaciones, animaciones interactivos, realidad virtual e incluso texto de mucha extensión o series de imágenes fijas, elementos que pueden tener mucha utilidad para capacitación y educación en línea. Pero la mayoría de usuarios de Internet, es muy probable que streaming termine identificándose con video. Los videos en línea pueden ser vistos

cuantas veces el usuario lo desee, también los puede pausar, adelantar o retroceder y ver a velocidad diferente a la normal.

- **TLS:** es un protocolo mediante el cual es posible crear un canal cifrado entre el cliente y el servidor. Así el intercambio de información (identificación de usuario y contenido de los mensajes) se realiza en un entorno seguro y libre de ataques pasivos. Es un protocolo criptográfico mixto (basado en cifrado simétrico y asimétrico), que utiliza certificados x509 y que es el utilizado por los servidores HTTP seguros.
- **UAProf:** Los perfiles de agentes de usuario describen las características de un terminal cliente y las preferencias configuradas para el despliegue de aplicaciones
- **WTLS:** Es la capa de seguridad de WAP, la cuál proporciona integridad y autenticación de los servicios, diseñado explícitamente para un entorno inalámbrico

Capítulo 6

Estandarización.
Soluciones de Proveedores comerciales para un Sistema DRM.

6. Estandarización y Soluciones de Proveedores Comerciales para un Sistema DRM.

Digital Rights Management es una tecnología que esta emergiendo en el mercado.

Un estándar es abierto si cualquiera que busca usarlo, pueda obtener acceso a este completamente, si esta controlado por un acceso publico en lugar de un vendedor, y si esta completo sin ambigüedades que sirve como base para la implementación.

Hay dos aspectos importantes para la estandarización de algunos aspectos de la tecnología DRM, el primero es tener en consideración que toda la actividad ahora del mundo de DRM esta pensada para Internet, segundo los estándares que deberán cubrir aquellos aspectos de los proveedores de contenidos.

Las principales integrantes de un sistema DRM son: Los Componentes (como el empacador de contenidos, y el controlador DRM vistos en el capítulo 3 de un Sistema DRM general), protocolos, los formatos de los archivos, metadatos, y los esquemas de encriptado y marcas de agua.

Tecnológicamente los componentes como el empacador de contenidos y el controlador DRM no son buenos candidatos para la estandarización, porque los publicadores necesitan una fuerza de competitividad para estos componentes, los formatos de archivos tampoco puedes ser estandarizadas ya que ellos ahora ya están en formato estándar (html, pdf, rtf, gif, etc.)

Los metadatos son tal vez un área clave para la estandarización, los protocolos los cuales dependen fuertemente de los metadatos, son también un buen candidato.

La encriptación es otra materia, por ejemplo en Estados Unidos de Norteamérica están avanzados en un estándar de encriptación como el DES (incluye el RC5 y RC6 de la RSA Security) y el AES que es el sucesor del DES, el cual esta basado en un algoritmo belga.

Los metadatos son considerados altamente como un área para la estandarización, los cuales incluyen la identificación, los metadatos *discovery* y los derechos. La identificación de los contenidos es el más básico elemento de un sistema DMR, cada contenido deberá tener una identificación única. Varios segmentos de la industria de contenidos han inventado sus propios esquemas de identificación, muchos de los cuales son ligados a un tipo particular de publicaciones como por ejemplo el Internacional Standard Boork Number, (ISBN) que es usado para copias impresas de libros y productos relacionados, el Internacional Standard Serial Number (ISSN) usado para series de copias impresas, como revistas, periódicos, el Librery Of Congress (LOC) número utilizado para los libros publicados en Estados Unidos. Ninguno de esos esquemas de identificación fue dirigido para ser usados en contenidos en

línea. En Internet se está pensando en un Digital Objet Identifier (DOI), que inicio en 1994, como parte de una iniciativa de administración del derecho de copia en línea *copyrigt on line*, con la asociación de publicadores americanos. La iniciativa comenzó como una ayuda para encontrar caminos de estandarización para resolver el problema de la administración del *copyright on line*. Este tiene limitaciones cuando es usado para identificar piezas de propiedad intelectual. Otro tipo de identificador que fue desarrollado para un mundo en línea es el Publisher Item Identifier (PII), este ha sido establecido por un grupo de publicadores científicos, pero este ha cedido su paso al DOI. La ITEF ha considerado construcciones llamadas Uniform Resourse Name (URN) y Persistent Uniform Resourse Locutor (PURL), ambas son similares al DOI, por lo tanto DOI tiene un alto potencial como un estándar abierto para identificación de contenidos en arquitecturas de DRM.

6.1. Tecnología XrML

Los esquemas de los metadatos de los derechos pueden ser estandarizados mediante la adopción de un modelo de derechos. Un estándar de modelo de derechos es el Extensible Rights Markup Language (XrML), un modelos de derechos del subconjunto útil esta comprendido en el protocolo Information and Content Exchange (ICE) comercia con una asociación de contenidos de negocio a negocio, los estandares más reciente como el MPEG para audio y video multimedia incluyen relatos para el modelado de derechos y herramientas para la administración de derechos, aunque ellos no especifican la información de los derechos por sí mismos, MPEG-7 también incluye información sobre los derechos, pero no en detalle.

Extensible Rights Markup Language (XrML) para la construcción de especificación de derechos tuvo su origen en el trabajo que el doctor Mark Stefik realizo en los laboratorios de Xeroxs Parc a mediados de los 90's, y fue quien invento el lenguaje Digital Property Rights Language; Stefik trabajo dirigiéndose en su concepto de sistemas fiables. La idea de Stefik es que cualquier tipo de sistema fiable podrá ser construido de tal forma que pueda leer especificaciones escritas en un cierto lenguaje y actuar de acuerdo a ellas. El originalmente imagino un sistema fiable de dispositivos de hardware pero en realidad puede ser un software de DRM en una PC. Otro importante concepto de la investigación de Stefik es que el sistema de almacenamiento digital, el cual es una colección de documentos en el cual se incluyen ambos el contenido tal vez en forma cifrada y la especificación de los derechos. En la

experiencia de Stefik se incluye la búsqueda de lenguajes orientados a objetos el estuvo diseñando una versión de un lenguaje de programación orientado a objetos LISP.

Xerox Corp. Patento DPRL, comenzó a comercializar DPRL, formando una unidad de negocios llamada Xerox Rights Management, desarrollo una tecnología DRM comercial en función del DPRL y creo una segunda versión de DPRL usando sintaxis de XML. A principios del 2000 Xerox giro bruscamente y la unidad que había creado se separo de la compañía y formo una empresa llamada Content Guard Inc tomo toda las propiedades intelectuales de Xerox Rights Management incluyendo la patente de DPRL, la cual fue modificada y renombrada a XrML.

XrML es un rico lenguaje, con complejidad equivalente a el lenguaje de programación SQL, no es un lenguaje de programación es una especificación del lenguaje. Esto es permitirles a los programadores especificar la forma o la estructura de algún objeto en detalle sin tener que especificar como esta estructura es actualmente implementada. Permite a los programadores especificar en que manera se comunican los sistemas fiables con otros sistemas fiables o con el mundo exterior (dispositivos de salida) en términos de la ejecución de los derechos.

Para implementar XrML se necesita desarrollar un intérprete para el lenguaje, el cual es una pieza de software que toma comandos en XrML y hace que ellos se ejecuten en un dispositivo. Un dispositivo que soporta XrML podrán aceptar archivos escritos en lenguaje y entender como se manejan de igual forma como un dispositivo de impresión postscript puede interpretar archivos postscript.

Por ejemplo, XrML tiene maneras para definir derechos en un contenido como reproducir y /o copiar un interprete XrML debe traducir el derecho de reproducir en un código que realmente reproduzca el contenido en el dispositivo, cuando el derecho es invocado.

Una tecnología escrita en XrML es llamado documento, es en realidad un conjunto de metadatos. La parte más importante de un documento XrML es la componente *work*.

El componente *work* incluye la información de los derechos del contenido y otros metadatos, contiene los siguientes subcomponentes:

- `OBJECT:` Es el nombre del trabajo y un ID el cual puede ser un DOI, ISBN, u otro tipo de identificador.
- `DESCRIPTION:` Es una descripción opcional del trabajo principalmente para ser más entendible a las personas

- CREATOR: Es una descripción del creador del trabajo, el cual puede ser un autor, un fotógrafo o un compositor
- OWNER: Permite al creador del documento XrML especificar de forma opcional quién está autorizado ha hacer cambios a los derechos del contenido.
- DIGEST: Es un valor criptográfico similar a la firma digital, que permite a el creador verificar la integridad del contenido actual, a diferencia de la firma digital la cual ayuda a verificar la integridad de la estructura del documento XrML.
- PARTS: Permite al creador del documento XrML especificar que otros trabajos están incluidos como parte de un trabajo de que este documento XrML le describe.
- CONTENTS: Describe la parte del contenido actual, el cual se le aplican las especificaciones de los derechos. El modo en que CONTENTS es descrito depende del contenido que este sea; puede ser expresado en bytes, Society of Motion Picture and Televisión Engineers (SMPTE), códigos de tiempo, etc.
- COPYES: Describe el numero de copias del contenido el cual el derecho describe; si es omitido, se asume que el número es uno. Esto es importante ya que influye en los derechos de transporte. Si hay dos copias del contenido y el usuario ejecuta un derecho de préstamo, para prestar una copia a otro usuario, una segunda copia permanece para el usuario para usarla mientras la primera es enviada como préstamo.
- COMMENT: Es un campo de texto reservado para comentarios, típicamente escrito por la persona o aplicación que crea el documento XrML.
- SKU: Es de utilidad para los distribuidores de contenido digital, este les ayuda a relatar el contenido hacia otras variables necesarias para venderlo que pueden ser llaves criptográficas o cupones de descuento.

6.1.1. Especificación de los derechos de uso.

RIGHTSGROUP (O REFERENCEDRIGHTSGROUP): Especifica derechos para el *work* pueden ser bastantes para cada documento

RIGHTSSGROUPS puede tener nombres como por ejemplo estándar, suscipción, estudiante etc. el componente principal es RIGHTSGROUP es RIGHTSLIST.

RIGHTSLIST encubre los derechos de modelado de XrML, a continuación se enlista los derechos que soporta:

- **Derechos de Suministro:** PLAY, PRINT, EXPORT y VIEW.

- **Derechos de Transporte:** COPY, TRANSFER, y LOAN.
- **Derechos de Trabajo Derivados:** EDIT, EXTRACT y EMBED.
- **Derechos de administración de archivos:** BACKUP, RESTORE, VERIFY, FOLDER, DIRECTORY y DELETE.
- **Derechos de Configuración:** INSTALL y UNINSTALL.

Cada derecho en RIGHTSLIST tiene un conjunto de términos y condiciones asociadas con él, consisten en el control del acceso, el período de tiempo, la geografía, y consideraciones asociadas con la ejecución del derecho.

6.1.2. Tipos de derechos.

PLAY significa crear un efímero suministro de el contenido, uno que se va cuándo el contenido esta terminado, cuando se ha terminado, VIEW es un sinónimo de PLAY pero este se puede aplicar cuando un contenido digital el termino *play* no es utilizado como en el caso de las imágenes. PRINT significa crear un *permanente* suministro del contenido en algún medio de salida, como una copia impresa. EXPORT significa pasar el contenido fuera de un sistema fiable. COPY significa crear una nueva copia de el documento XrML. TRANSFER significa mover el documento XrML desde un sitio de almacenamiento a otro y LOAN crea una copia temporal del documento y la mueve a otro sitio de almacenamiento por un periodo especifico de tiempo, durante la original copia esta usándose. Cada uno de éstos tiene una cláusula opcional llamada NEXTRIGHTS el cuál habilita la Superdistribución, este describe los derechos que son sumados o borrados de una nueva copia del contenido.

EXTRACT da al usuario el derecho de tomar una porción del *work* y crear un nuevo *work* en cambio podrá ser incorporado en un *work* largo. El nuevo *work* que el derecho de EXTRACT crea es representado en otro documento XrML. EXTRACT tiene un opción que es EDITOR que permite especificar el tipo de software de edición que se podrá utilizar en la extracción, idealmente es otro sistema fiable que conoce como se crean documentos XrML.

Los derechos de EDIT y EMBED son variantes de EXTRACT.EDIT permite un valor agregado a la opción de cambio del contenido.

BACKUP y RESTORE permite hacer respaldos de documentos para un fin explicito de restauración si el documento originalmente tiene un problema.

6.2. ODRL (Open Digital Right Language)

El Open Digital Rights Language (ODRL) proporciona la semántica para expresiones DRM en ambientes abiertos y fiables.

El Open Digital Rights Language (ODRL) proporciona la semántica para un lenguaje de expresión para Administración de Derechos Digital y el diccionario de datos que pertenece a todas las formas de contenido digital. El ODRL es un vocabulario para la expresión de términos y condiciones sobre el contenido digital que incluye permisos, restricciones, obligaciones, condiciones, y acuerdos con los titulares de los derechos. El ODRL es colocado para ser ampliado por diferentes sectores de industria (como ejemplo libros electrónicos, música, audio, móvil, software) y ser un lenguaje de interoperabilidad principal y que no tiene ningún requerimiento de licencia.

Los Partidarios de la iniciativa de ODRL creen en la filosofía de un estándar abierto para Lenguaje de Derechos y la promoción de tales ofertas de estandarización y la amplia aceptación a través de las comunidades de DRM

6.3. Soluciones de Proveedores para DRM-Rich.

A continuación se describirán y analizarán algunas soluciones particulares que ofrecen dos importantes fabricantes de software y de terminales móviles, la empresa Microsoft con el software Microsoft ® Windows Media™ Rights Manager para acceso de tipo fijo y contenidos de costo de creación y distribución elevados y la empresa Nokia para acceso de tipo inalámbrico y contenidos de bajo costo.

6.3.1. Windows Media con DRM.

Primeramente se analizará el tipo de atacantes a los contenidos digitales, éstos pueden distinguirse como pertenecientes a una de estas tres categorías: ingenuo, experto y profesional.

- Un atacante ingenuo activamente no intenta romper un sistema DRM pero copiará archivos e instalará aplicaciones hackeadas. El objetivo de esta tecnología para este caso es parar al atacante ingenuo dándole vuelta o bordeando al sistema DRM.
- Un atacante experto sabe sobre computadoras y software pero no tiene ninguna motivación comercial para romper un sistema DRM. El objetivo es de hacerle más difícil y costoso para un atacante experto corromper un sistema DRM.

- Un atacante profesional es motivado comercialmente a violar un sistema DRM con fondos para montar otros ataques y también alquilando a otros hackeres. El objetivo en este caso es de reducir al mínimo el alcance de las violaciones y limitar las oportunidades comerciales.

El Administrador de derechos de Windows Media (Microsoft ® Windows Media™ Rigths Manager) es una aplicación de administración de derechos digitales que permite que los autores de contenido entreguen canciones, vídeo y otros contenidos multimedia a través de Internet con un formato de archivo empaquetado y cifrado. Los usuarios finales necesitan aparte una licencia con la clave que descifra el archivo para poder reproducirlo en el Reproductor de Windows Media.

El Administrador de derechos de Windows Media utiliza un esquema de cifrado de alto nivel para la administración de los derechos digitales. Todos los archivos son almacenados en un formato de cifrado exclusivo para cada equipo, que tenga y ejecute Windows, lo que hace que resulte muy difícil hackear la licencia o copiar el archivo. El esquema de cifrado de "equipo a equipo" basado en Windows protege a los consumidores frente a la sustracción involuntaria de archivos. También actúa como medida disuasoria frente a la piratería intencionada.

También usa tres características diferentes:

- La Distribución Segura de archivos Multimedia de Windows
- Un modelo de negocio flexible.
- Una plataforma altamente escalable.

6.3.1.1. La Distribución Segura de archivos Multimedia de Windows

- **Protección persistente: WMRM** "cierra" archivos de Multimedia de Windows con una llave de licencia para mantener el contenido protegido, aunque estos archivos sean extensamente distribuidos. Cada licencia únicamente es asignada a cada computadora. Esto previene la distribución ilegal de archivos de Multimedia de Windows.
- **Un Cifrado Fuerte:** incluye los esquemas de cifrado probados. Técnicas estándar criptográficas son usadas para autenticar componentes y proteger contra atacantes que violan al código y a los datos. La Autenticación de los componentes DRM

permitidos es alcanzada usando firmas digitales y certificados de claves públicas. La curva Elíptica y algoritmos RSA son usados para autenticar componentes que usan firmas digitales y realizan operaciones de cambio de llaves para el establecimiento de canales seguros entre componentes.

- **La revocación:** La revocación es un proceso que identifica los certificados de aplicaciones quebrantadas, violadas o hackeadas, y previene a estas aplicaciones de reproducir archivos empaquetados. Cada licencia que es emitida por un servidor en el cual esta ejecutándose WMRM contiene una lista de revocación. La revocación ayuda para prevenir una ruptura global de un sistema DRM y limita la oportunidad comercial para un atacante profesional por la implementación de los consumidores a comprometerse a actualizar el software para la reproducción de nuevos contenidos digitales.
- **La individualización:** Hace que el software instalado sobre una PC de un usuario sea totalmente diferente a comparación de las PC's de otros usuarios. El resultado es que si el software individualizado es hackeado o violado, sólo aquella versión se verá afectada, así se logra eliminar violaciones globales en la aplicación y se logra que los ataques sean más difíciles y costosos para el violador.

  Los dueños de los contenidos pueden usar esta característica como un requerimiento y los consumidores deberán usar el software de reproducción individualizado para poder reproducir sus archivos empaquetados, aunque dentro del software se puede incorporar la individualización como un paso durante la instalación. Cuando este proceso es iniciado, el software envía una petición al Servicio de Individualización de Microsoft sobre Internet, el servicio genera un DLL único que es confuso y es digitalmente firmado, luego lo liga a la PC del cliente usando su ID del hardware. Las técnicas estándar criptográficas son usadas para autenticar componentes y proteger contra atacantes que sabotean el código y los datos.
- **Los componentes de Autenticación:** Es alcanzada usando firmas digitales y certificados públicos claves. En el cifrado y en los procesos de desciframiento se usa un código simétrico basada en RC4 y estándares de cifrado DES, el cuál ha sido publicado en la Eurocripta 98, este algoritmo es rápido; se puede cifrar y descifrar unidades de datos a una tasa de 10 MB por segundo.

- **Patrones seguros de audio:** actualmente únicamente es soportado por Windows Me, proporciona una infraestructura a nivel Kernel para el mantenimiento de la protección de los derechos de autor ayudando para asegurar que los datos de audio llegan a la tarjeta de audio a una PC y no son desviados a un programa no autorizado. Los patrones Seguros de audio están planeados para ser en un futuro un rasgo del sistema de operaciones de Microsoft. Los dueños de Contenidos usan esta característica por requerimiento de patrones seguros de audio para sus archivos empaquetados, controlando así el uso de patrones seguros de audio por la licencia para el archivo empaquetado.

  Los patrones seguros de audio trabajan con la creación de un canal seguro entre el componente DRM del software del reproductor y el componente DRM del kernel. El dueño de los contenidos puede requerir los componentes que reciben la señal descifrada de audio para ser certificada por Windows Hardware Quality Labs. El Ruido es agregado a la señal, y removido antes de que alcance la salida del dispositivo. La salida digital sobre este dispositivo puede ser inutilizada si el dueño del contenido lo requiere.

La release actual, Windows Media Rights Manager versión 7, incluye software development kits (SDKs) para ambos cliente y servidor que permite a las aplicaciones proteger y reproducir archivos Multimedia de Windows. El cliente SDK es parte de Windows Media Format SDK, mientras que el servidor SDK es llamado Windows Media Rights Manager SDK.

Usando WMRM versión 7 SDK, los desarrolladores pueden crear aplicaciones que cifran (empaquetan) archivos de Multimedia de Windows y emiten licencias para aquellos archivos de Multimedia de Windows. Un archivo empaquetado con Media Windows contiene una versión del archivo que ha sido cifrado para que solo la persona que ha obtenido una licencia para aquel archivo pueda reproducirlo. La licencia está separada del paquete de Media Windows, lo que significa que el contenido y la licencia para aquel contenido pueden ser adquiridos en diferentes tiempos. Los archivos Cifrados pueden ser descargados o transferidos o por streming a la PC del cliente.

Hay 250 millones de PC (Windows y Macintosh) reproductores en uso, y más de 70 dispositivos diferentes incrustados que soportan Windows Media Rights Manager (reproductores portátiles de audio, reproductores de CD etc.)

6.3.1.2. Modelo de negocio flexible

Nuevas licencias de Derechos han sido introducidas en WRMW que ayudan a la creación de nuevos modelos e innovadores modelos de negocio.

- **Licencias y Contenidos Digitales Distribuidas Separadamente.**
  Las licencias son emitidas independientemente de los archivos de Multimedia de Windows, proporcionando una máxima flexibilidad y así mismo permitiendo una amplia distribución del contenido. Cada vez que un archivo de Multimedia de Windows es reproducido, el Administrador de Derechos comprueba si la PC del consumidor tiene una licencia. Los consumidores que no tienen una licencia válida son dirigidos a una página de registro de licencia.
- **Condiciones del Licenciamiento easy-to-Change**
  Como las licencias y archivos de Multimedia de Windows están almacenados separadamente, las condiciones del licenciando puede ser cambiado en el servidor, sin tener que redistribuir o de empaquetar de nuevo el archivo de Multimedia de Windows.
- **Modelo de Suscripción**
  Los proveedores de contenido pueden controlar el inicio de una licencia, la finalización, y la duración de la misma para crear modelos innovadores de negocio. La utilización de estos diferentes derechos permite a proveedores de contenido optimizar sus propias reglas de negocio.
- **Reproducción de Vistas Previas Limitadas.**
  Usando las operaciones contadas en la opción (de repetición) en la estructura de una nueva licencia, los proveedores de contenidos puede crear licencias de alquiler o de "preview" para la inspección de archivos de Multimedia de Windows.
- **Licenciamiento Transparente.**
  Una característica como el "predelivery" (pre-entrega) de licencias y el licenciamiento silencioso mejoran la experiencia del consumidor con archivos quitando las barreras para la adquisición y reproducción de archivos de Multimedia de Windows seguros. El licenciamiento silencioso significa que un proveedor de contenido puede entregar la licencia al consumidor sin la necesidad de que el consumidor tenga que solicitar más información.

- **Transferencia Controlada a Dispositivos SDMI Portátiles**
  Windows Media Device Manager garantiza una transferencia segura de archivos Multimedia de Windows protegidos por Secure Digital Music Iniciative (SDMI) en dispositivos portátiles.

6.3.1.3. Plataforma Sumamente escalable

Es una tecnología sumamente escalable lista para su implementación para medianos a grandes aplicaciones de comercio electrónico.

- **Fácil Integración**
  La publicación de Application Programming Interfaces (APIs) son fácilmente integrados con soluciones de comercio electrónico existente.
- **Licenciamiento de Volúmenes grandes**
  La entrega de volúmenes grandes de licencias, puede entregar 500,000 licencias por día un solo servidor.
- **High-Volume Media File Packaging**
  Un solo servidor puede proteger más de 500,000 archivos de música por día.
- **COM – based Platform.**
  Objetos (COM) son usados para proteger archivos de Multimedia de Windows y las licencias en cuestión, permitiéndole integrar el proceso de adquisición de licencia con su actual modelo de negocio.

6.3.1.4. Como Windows Media Rights Manager Trabaja

El proceso de distribución protegida de archivos Multimedia de Windows con WMRM es esquematizado dentro de cinco áreas:

- Creación de contenido digital y posterior codificación a un formato de Windows Media.
- Empaquetado de archivos basados en Windows Media.
- Distribución de los archivos empaquetados a los consumidores
- Generación y emisión de licencias
- Reproducción de archivos empacados y administración de licencias.

La figura de abajo ilustra el proceso.

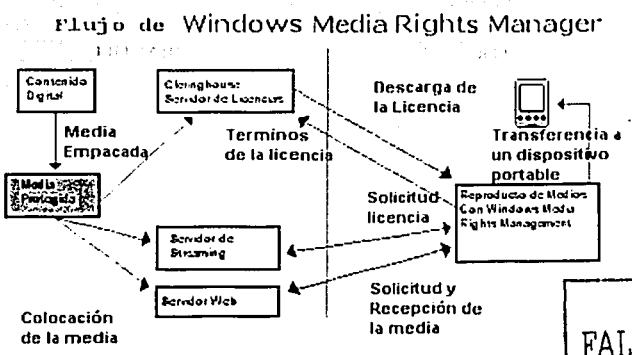


Figura 6.1 Proceso para la protección de contenidos con formato de Windows Media en una plataforma de Windows

6.3.1.5. Empacado de los archivos Multimedia de Windows.

La creación y la codificación del contenido digital están en realidad fuera del alcance de WMRM, pero éste es el primero paso en el proceso.

Los dueños de los Contenidos primero capturan el contenido de audio o de vídeo en un formato digital, y después lo codifican en un formato de Windows Media, usando una herramienta que es el Windows Media Encoder. Por motivos de seguridad, sólo los codecs DMO son soportados y autorizados; los archivos creados con los codecs ACM no pueden ser reproducidos. Una vez que los archivos Windows Media han sido creados el siguiente paso será empacarlos.

El empacado de un archivo implica la creación de una llave y la cabecera del contenido, y el cifrado del archivo con la llave.

WMRM usa algoritmos de cifrado muy fuertes y hacen comprobaciones de integridad en tiempo de ejecución. El proceso es rápido más de 540 KB por segundo. Todos los paquetes de carga útil son cifrados individualmente pero el aumento es mínimo.

Una llave es generada por medio de un algoritmo que usa un ID llave y una semilla llave de licencia. El ID llave es un valor que por lo general es generado separadamente para cada contenido. La semilla llave licencia es un valor usado por una organización para empaquetar

todos sus archivos. Por ejemplo, para empacar 100 canciones, un estudio de grabación crea 100 IDs de llaves, luego se usa la semilla llave licencia para generar 100 llaves.

A veces una llave puede ser usada para múltiples archivos (tal como una llave puede abrir más de una puerta). Algunos archivos que comparten una llave también comparten una licencia. Por ejemplo, una licencia podría ser usada para 10 canciones diferentes de un álbum. Sin embargo, la seguridad es más grande y los esquemas de licenciamiento son más flexibles cuando una llave diferente es usada para cada archivo empacado.

El diagrama siguiente muestra el flujo de información que resulta de empacar un archivo de Windows Media

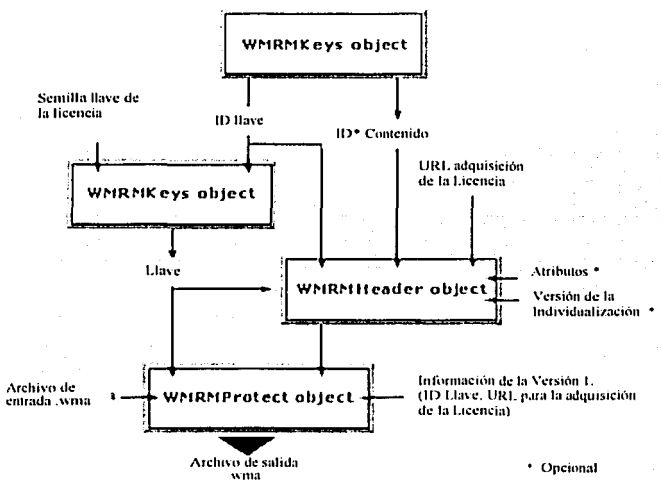


Figura 6.2 Diagrama que esquematiza el empacado de un contenido así como la generación de la llave para el cifrado.

Un archivo de Windows Media es empaquetado usando el procedimiento siguiente:

1. Se utiliza el objeto de WMRMKeys para generar un identificador ID de la llave y un identificador ID del contenido.
2. Se utiliza el objeto de WMRMKeys con la semilla de la llave de la licencia y el ID de la llave para generar una llave.

3. Se utiliza el objeto de **WMRMHeader** con la llave, el ID de la llave, el ID del contenido, y el URL para la adquisición de la licencia para crear la cabecera del contenido. Se recomienda que sean agregadas cualidades y especificar opcionalmente el número de versión solicitada para la individualización.
4. El objeto **WMRMProtect** con el archivo de entrada, la llave, y la cabecera del contenido para producir los archivos de Windows media empaquetados.

El ID de la llave es una cadena de caracteres usada para generar la llave. Más tarde, el emisor de licencia usará este ID llave para regenerar la llave que se incluirá en la licencia. El ID del contenido es un valor único que identifica cada archivo empaquetado. Por ejemplo, este valor puede ser almacenado en una base de datos como la llave primaria con el correspondiente ID de la llave y metadatos.

Una adquisición de licencia URL indica la página de Web que es el principio del proceso para la adquisición de la licencia. Cuando una licencia válida no se encuentra para un archivo, el software del reproductor abre este URL. Por ejemplo, la página informaría a los consumidores que necesitan una licencia, con información extra (como por ejemplo: cuanto cuesta esto o lo que la licencia le permite hacer).

El número de versión de la individualización, cuando es especificada, requiere que el consumidor esté usando una aplicación de un reproductor individualizado con una versión mínima. Si el consumidor está de acuerdo, el proceso de individualización comienza; si no, el archivo no puede ser reproducido.

Los atributos, que son opcionales son pares de valores de nombres, son usados para añadir información extra al cliente en un archivo empaquetado, tales como el dueño del contenido, el artista, el título, etc. Esta característica es útil cuando múltiples partes administran archivos en un sistema WMRM permitiéndoles comunicar y rastrear la información sobre el archivo. Por ejemplo, el siguiente atributo podría ser usado para ayudar al emisor de licencias a determinar el distribuidor que vendió el archivo: WMRMHeader.Atributo ("Content_Dist") = "Company X"

Una vez que la cabecera ha sido creada se debe firmar digitalmente para aumentar seguridad y evitar que sea corrompida el archivo WMRM empaquetado. La cabecera del contenido se firma con llave privada del usuario; ya que el emisor de la licencia es el que verifica la firma, el usuario debe compartir su llave pública con el emisor de la licencia. Antes de la emisión de una licencia, el emisor de la licencia debe verificar la validez de la firma de la cabecera

usando la llave pública del empaquetador del contenido. Si estas firmas no son iguales, la licencia no se publica.

Por ejemplo, si alguien intentara cambiar la identificación del contenido en un archivo de Windows Media, la firma de la cabecera del contenido sería corrompido, indicando que el archivo de Windows Media fue tratado de forzar.

El código siguiente de Visual Basic Scripting Edition muestra como fue desarrollada una cabecera del contenido.

```
HeaderObj.KeyID = key_id
HeaderObj.LicenseAcqURL = laurl
HeaderObj.ContentID = content_id
HeaderObj.IndividualizedVersion = indiv_version
' The following attributes are recommended.
HeaderObj.Attribute("Copyright") = "copyright statement"
HeaderObj.Attribute("Content_Type") = "audio or video"
HeaderObj.Attribute("Author") = "artist name"
HeaderObj.Attribute("Artist_URL") = "http://artist_web_site"
HeaderObj.Attribute("Title") = "title"
HeaderObj.Attribute("License_Dist") = "name of license issuer"
HeaderObj.Attribute("License_Dist_URL") = "http://license_issuer_web_site"
HeaderObj.Attribute("Content_Dist") = "content distributor"
HeaderObj.Attribute("Rating") = "rating"
HeaderObj.Attribute("Description") = "description"

call HeaderObj.SetCheckSum(key)
call HeaderObj.Sign(privatekey)
header = HeaderObj.Header
ProtectObj.Header = header
```

Ejemplo VBScript de una cabecera para el contenido

6.3.1.6. Generación y Emisión de Licencias.

Las licencias son generadas y emitidos usando el Servidor de Licencias de Windows Media, el cual es un componente de WMRM que corre sobre un servidor. La licencia es ligada a la PC para la cual esto es emitido, entonces un archivo empaquetado puede ser compartido, pero una licencia no podrá compartirse. Como la licencia es el elemento vital, esto hace el sentido de ligar el pago a la seguridad de la licencia. Es decir los archivos empaquetados pueden ser distribuidos libremente, pero la distribución de licencia debería ser más cuidadosamente controlada. Por ejemplo, una tienda de música en linea podría permitir a los clientes descargar y compartir archivos empaquetados, pero cobraría honorarios por las licencias para que puedan ser reproducidos aquellos archivos.

controlada. Por ejemplo, una tienda de música en línea podría permitir a los clientes descargar y compartir archivos empaquetados, pero cobraría honorarios por las licencias para que puedan ser reproducidos aquellos archivos.

Las licencias agregan más seguridad a un Sistema WMRM. El Windows Media License Service podrá verificar la firma de la cabecera de un contenido de un archivo empaquetado para asegurar esto no ha sido quebrantado. Además, la licencia usa un estado seguro para almacenar la información. Por ejemplo, si una licencia tiene una fecha de vencimiento, un derecho puede ser configurado para invalidar la licencia si el reloj de la PC es cambiado.

Una licencia contiene la siguiente información:

- La llave para abrir o descifrar el archivo empaquetado. Esta llave es regenerada usando ID de la llave del archivo empaquetado y la llave semilla de licencia. Si el emisor de licencia no es la misma organización quien empaqueto el archivo, la llave semilla de licencia debe ser compartida.
- Los derechos o reglas y las condiciones de la licencia, los cuáles son definidos usando XML-based event-driven rights language. Soportan una gran gama de diferentes reglas de negocio, las cuales incluyen:
    - Cuántas veces puede ser reproducido un archivo.
    - Los archivos que pueden ser transferidos o reproducidos en que dispositivos. Por ejemplo, los derechos especificarán si el cliente podrá transmitir el archivo a dispositivos portátiles que son compatibles con Secure Digital Music Initiative (SDMI).
    - Cuando el usuario puede empezar a reproducir el archivo y cuando es la fecha de expiración.
    - Si el archivo puede ser transferido a un CD (quemado).
    - Si el usuario puede hacer una copia de seguridad de la licencia, etc.
- La Prioridad de la licencia en lo que concierne a otras licencias para el mismo archivo de Multimedia de Windows (es posible emitir licencias múltiples para un mismo archivo).
- Atributos del cliente (nombre/ pareja de valores) como una descripción de la licencia.

La configuración de los derechos es uno de los pasos en la generación de una licencia, y pasa de diferentes formas según el modelo de negocio. Los derechos pueden ser puestos en marcha. Por ejemplo, si a los consumidores se les da una opción para pagar más, para obtener

el derecho de transferir archivos a dispositivos portátiles, los derechos serían puestos después de que esta opción esté hecha. Los derechos también pueden ser puestos en acuerdo, con el dueño del contenido. El emisor de licencia podría almacenar los ID's de los contenidos en una base de datos con los derechos que se dan para cada uno. El dueño del contenido también podría comunicar que derechos puede ofrecer incluyendo la información, como un atributo en la cabecera del contenido.

Las licencias pueden ser entregadas a consumidores de formas diferentes y en puntos diferentes de la transacción, según el modelo de negocio. El método usado para la emisión de licencias deberá conducir situaciones diferentes, como por ejemplo cuando el consumidor usa el software del reproductor anticuado o los reproductores que no soportan la adquisición de una licencia silenciosa. Los consumidores también pueden adquirir archivos de WMRM empaquetados de sus amigos, entonces el modelo debería conducir el caso de que cuando un consumidor intenta reproducir un archivo empaquetado sin una licencia.

Método Pre-entrega (predelivery)

- La entrega de licencia puede ser iniciada por el emisor de las licencias o por la aplicación del reproductor del consumidor.
- La licencia puede ser emitida antes de que el consumidor intente reproducir el archivo empaquetado, por lo general antes de que el archivo empaquetado sea descargado, o en el mismo momento.
- Cuando el consumidor reproduce el archivo, la licencia está ya en la PC del consumidor y el archivo puede ser reproducido inmediatamente sin una conexión a Internet.

Por ejemplo, un consumidor visita un sitio de Web donde se vende música y selecciona dos canciones para comprar. Después de haber efectuado el pago, dos licencias son emitidas (rápidamente y desconociendo al consumidor), entonces el consumidor es direccionado para que pueda descargar las canciones. Cuando el consumidor intenta reproducir el archivo empaquetado sin una licencia, el software del reproductor abre la URL para la adquisición de licencia y envía una solicitud de licencia. Esta petición contiene la cabecera del contenido, la información del cliente y la solicitud de los derechos del software del reproductor.

Estas licencias pueden ser emitidas de formas diferentes: **silenciosamente, no silenciosamente, o basadas en la plataforma del consumidor**. Cuando una licencia es emitida silenciosamente, significa que es emitida sin que el consumidor sea consciente de la

dirección de correo electrónico. Este método es útil cuando se quiere asegurar que el consumidor ve la información como las condiciones de la licencia.

Cada solicitud de licencia de un reproductor incluye la información de plataforma. Ciertas plataformas Windows Me o Windows XP proporcionan mecanismos de seguridad integrados, entonces se pueden emitir diferentes licencias basadas en la plataforma del consumidor.

En la siguiente figura observamos el proceso de empaquetado y emisión de licencias, así como la reproducción de los archivos.

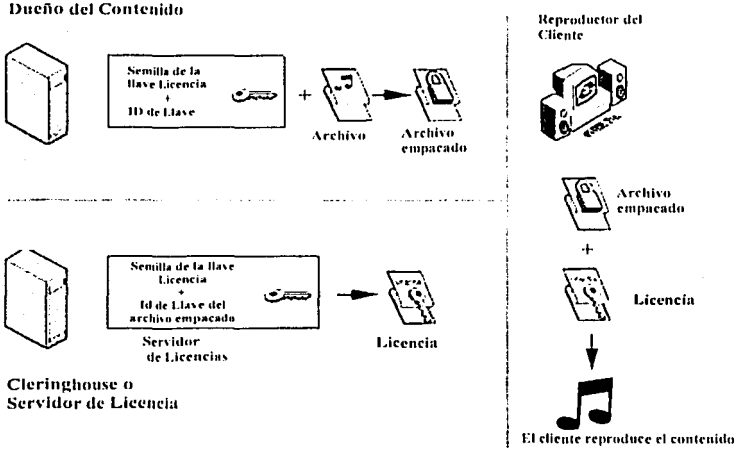


Figura 6.3 Generación de llave para cifrar el contenido y emisión de su respectiva Licencia para su posterior uso y reproducción del contenido protegido.

6.4. DRM-Lite de Nokia

La estructura existente y los papeles del contenido en los negocios deberían ser la base para la tecnología futura para DRM móvil. Los tonos de timbrado e iconos forman la mayor parte del negocio de los contenidos hoy en las redes móviles.

La infraestructura de DRM móvil está basada en los siguientes principios claves:

- El contenido y los derechos están separados (pero éstos pueden ser entregados en forma conjunta si se desea)
- El contenido es empacado dentro de Mobile DRM Container **MRCC**
- El uso de las reglas está expresado en un *Voucher*, usando un Lenguaje de Expresión de Reglas **MRV**
- Un Mobile DRM Container (MRCC) podrá ser referenciado por un número diferente de *vouchers* (vista previa, todos los derechos, etc).
- El uso de reglas está descrito en el *Voucher*, el cual se implementará por el middleware del teléfono móvil.

Los componentes claves en DRM móvil pueden ser descritos con la arquitectura siguiente:

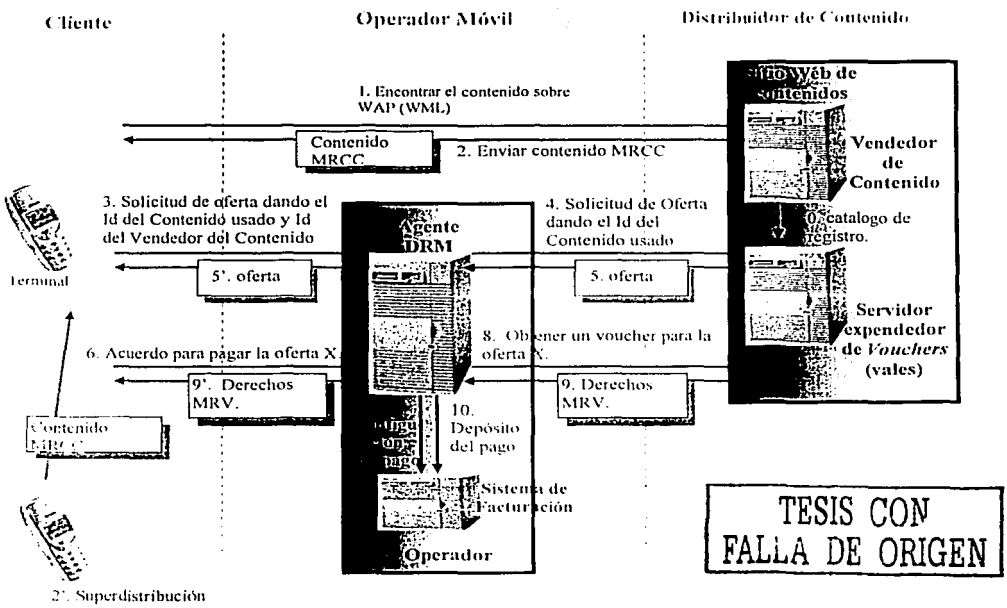


Figura 6.4 Arquitectura propuesta por Nokia para DRM móvil.

- **El Servidor expendedor de *Vouchers* o vales o *Voucher Server* (VS)** puede ser un *host* que pertenezca al proveedor de contenidos o un operador que juegue el papel de un proveedor de contenido. El tiene todos los registros VS de los contenidos en un sistema móvil DRM y los *vouchers*.
- **El Vendedor o expendedor de contenidos o *Content Server* (CS)** es un *host* para el proveedor de contenido o sus socios de contenidos si es que está funcionando en un modo de agregación. En el CS incluye la descarga de contenido.
- **El Agente DRM o *DRM broker*** es un *host* para la recolección del pago, el cuál podría ser también el operador. El broker es efectivamente un "Rigths-clearing feature" de una solución de pago móvil con interfaces a sistemas de pagos.

En este ejemplo, el proveedor de contenidos (el VS y el dueño CS) hace un pago y los derechos al cleringhouse en acuerdo con el operador, sosteniendo un convenio para pagar un cierto porcentaje sobre cada transacción ejecutada. El VS del proveedor de contenidos mantiene la pista de todo el contenido que esta puesto en circulación por la red. El dueño CS debe registrar cada objeto que ellos quieren transferir a un sistema móvil DRM. El método para el registro del contenido, es en esencia, que el CS es embarcado en el contenido en el VS, que crea un ID de contenido único y embala o empaca el contenido en un paquete específico DRM. Además, el CS cuenta con el VS que nos dice qué clase de reglas de uso puede ser emitido para el contenido.

El ver y transferir los registros de contenido ocurre directamente entre el CS y el consumidor, independientemente del proceso de compra del vale. Una vez transferido, el contenido registrado puede fluir libremente de terminal a terminal. Cuando el usuario intenta reproducir el contenido registrado, la terminal comprobará si hay un vale con el contenido que se refiere ID en el terminal. Si no hay tal vale, la terminal iniciará un proceso de pago y derechos limpios con un proveedor de servicio de pago.

La compra de vale es realizada por el broker de DRM, basado en la dirección del VS. Una vez que el consumidor acuerda pagar, el broker DRM limpia el pago y pregunta por el vale al VS. El proceso de ejecución de derechos es completado cuando el broker DRM re-envía el vale generado por el VS al usuario.

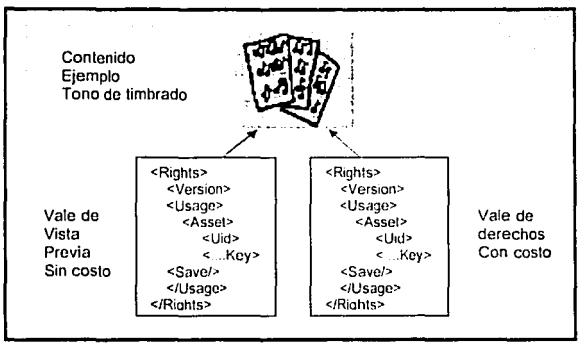


Figura 6.5 Ejemplo de la estructura de un vaucher (vale) con derechos móviles se esquematiza el vale de vista previa sin algún costo y después con todos los derechos y ya con un costo lo que permite salvar o comprar el contenido.

Capítulo 7

Conclusiones.

7. Conclusiones.

La finalidad de este trabajo escrito de Tesis es dar a conocer y entender este nuevo concepto de la Administración de Derechos Digitales como solución al problema surgido del uso no autorizado de bienes digitales a partir de la distribución, adquisición y reproducción de todos aquellos contenidos digitales que no están protegidos y que por lo tanto son extremadamente vulnerables a la piratería. En este capítulo dedicado a las conclusiones, en donde estas fueron organizadas por capítulo acompañadas de un breve descripción del mismo.

En el primer capítulo de esta tesis se describen todos aquellos servicios y aplicaciones basadas en IP que surgirán en la Tercera Generación de telefonía móvil la cual contara con mayores velocidades de Transmisión de Datos y una ancho de banda superior a las redes actuales de telefonía Móvil, el objetivo de este capítulo no fue hacer una descripción técnica de la evolución de las Redes Móviles actuales hacia la Tercera Generación ya que actualmente existen un conjunto notable de documentos y trabajos que nos puede orientar en este sentido el objetivo en sí de este capítulo radica en situarnos en un contexto donde se desarrollaran nuevas aplicaciones y servicios que probablemente se ajustarán a las necesidades y las elecciones individuales de los usuarios móviles y que por lo tanto los contenidos digitales utilizados o generados por dichas aplicaciones y servicios tendrán que ser protegidos para evitar su mal uso y su distribución indiscriminada.

Con la Tercera Generación de telefonía móvil se crearan nuevas gamas de servicios que estarán clasificados de la siguiente forma:

- Acceso a Internet Móvil: El usuario podrá tener acceso a cualquier servicio basado en IP.
- Acceso a las Intranets: Basándose en las capacidades técnicas para hacer uso de Internet Móvil, se podrá tener acceso seguro a Servicios Corporativos como Redes de Área Local-
- Infoentretenimiento Personalizado: El usuario podrá tener acceso a cualquier contenido que necesite independientemente de la terminal que utilice.
- De Multimedia: Se enfocan a un intervalo de aplicaciones que hacen uso de video y audio como por ejemplo: aprendizaje electrónico, comunicaciones corporativas, publicidad y mercadeo.
- Basados en localización: Se conocerá la ubicación del usuario y esto permitirá ofrecer información acerca de establecimientos comerciales cercanos, de rutas

alternativas en caso de incidencias viales, respuestas inmediatas a personas cuando soliciten auxilio, por mencionar algunas aplicaciones

- De Voz: El cual se mantendrá como clave para el desarrollo de las Operadoras Móviles, el cuál contara con servicios de valor agregado como videoteléfono.

La Tercera Generación tendrá éxito si cumple satisfactoriamente con las siguientes metas propuestas:

- Contar con una habilidad itinerante, es decir todos aquéllos servicios y aplicaciones en escenarios internacionales. Aquí observamos que se presentan algunas dificultades ya que se cuenta con una diversidad de estándares a nivel mundial y tecnológicamente va lento hacia una convergencia a la IMT-2000.
- Contar con un alto consumo de datos, reflejados en ingresos por la obtención y distribución de contenidos, sumados a los ingresos de la Operadora de Comunicaciones generados por la distribución del servicio. Se tiene la idea que con la creación de nuevos servicios y aplicaciones en función de su categorización se llegara a esta meta.

A fin de entender los Servicios y Aplicaciones basadas en IP que surgirán en la Tercera Generación de telefonía móvil es importante especificar algunas de las características técnicas del estándar móvil digital de Segunda Generación CdmaOne (IS-95 CDMA) y su evolución hacia la Tercera Generación.

CdmaOne evolucionara a cdma2000 convergiendo a IMT-2000.

Cdma2000 esta dividida de la siguiente forma:

Cdma2000 1X con un canal de 1.25 MHz de Ancho de banda a una velocidad de 144 kbps, la evolución más allá de 1X es llamado cdma2000 1xEV que será dividido en dos pasos 1xEV-DO (únicamente evolución de datos) y 1xEV-DV (evolución de voz y datos).

En resumen la implementación de Tercera Generación creara un nuevo canal para acceso a, información, distribución y ventas de contenido digital, esto proveerá una única oportunidad para los proveedores de contenidos que les generará nuevos ingresos.

En el segundo capítulo se realizó un seguimiento de cómo se han administrado los derechos de autor *copyright* (derechos de copia) de los diferentes tipos de propiedades intelectuales; como antecedentes y comprensión de la administración de derechos de autor en una etapa predigital y digital. Los derechos de autor están "protegidos" automáticamente desde el momento que se crea la obra, y una obra está "creada" desde que está plasmada en una copia o un archivo por primera vez. El concepto de derechos de autor es una forma de protección

proporcionada por las leyes para los autores de "obras originales" donde generalmente se le da al dueño de los derechos de autor el derecho exclusivo para hacer y para autorizar a otros a hacer lo siguiente: reproducir, preparar trabajos derivados, distribuir copias, interpretar, mostrar y presentar la obra públicamente.

Tomando como antecedente lo anterior, en este tema de tesis me enfoque a la administración de los derechos de autor en una era digital.

Inicialmente y en la actualidad se esta desarrollando el sistema para la distribución segura de los materiales/obras/creaciones con derechos de autor en Internet que protege y resguarda a los dueños de los contenidos de una piratería desenfrenada. Se observo que la industria ha empleado un amplio número de métodos técnicos y legales para impedir este proceso "liberalizador" de contenidos:

- La Administración de los derechos de Autor (*Digital Rights Management* DRM) aplicada por ejemplo en libros electrónicos intransferibles que permiten sólo un cierto número de lecturas.
- Códigos de protección en DVDs, haciendo uso de marcas de agua.
- Una nueva legislación como la UCITA (Uniform Computer Information Transaction Act), dentro del aspecto legal el cual es un proyecto de ley que regula los contratos relacionados con la información digital, en EE.UU pretende proporcionar un código normativo unificado que proteja las transacciones que involucren intercambios de programas e información, o aplicación estricta de la existente (como la persecución policial).

En este capítulo de la tesis, se obtuvo que un sistema DRM es importante ya que permite:

- Proteger la posesión de la propiedad intelectual, y controlar los derechos de los creadores/dueños de contenidos digitales del uso no autorizado.
- Asegura que los proveedores de contenido en particular los dueños de los derechos de autor reciban la remuneración adecuada por la creación de su contenido que es protegido con un sistema DRM.

Un Sistema DRM, propone una solución técnica esencialmente para:

- La protección de sus contenidos digitales al mal uso.
- La administración de aspectos comerciales, de propiedad intelectual y de confidencialidad.
- La distribución segura de los contenidos digitales con derechos de autor en Internet.

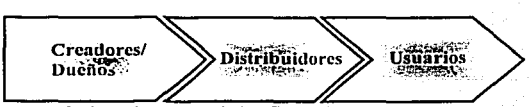
En este trabajo se han analizado dos formas distintas para la distribución de los contenidos digitales en línea acceso de tipo inalámbrico y fijo a Internet para ambos se clasificaron los siguientes modelos de negocio.

- Pago de Download (transferencia o descarga de archivos).
- Suscripciones.
- *Pay-Per-View y Pay-Per-Listen.*
- Superdistribución.

En el capítulo 3, se estudió el concepto y la arquitectura propuesta de un esquema general de la Administración de Derechos Digitales, así como los dispositivos de la misma.

Conceptualmente DRM es:

- Una cadena servicios y tecnologías de hardware y software que manejan el empleo autorizado de contenido digital y dirige cualquiera de las consecuencias derivadas de su empleo (administra las acciones resultantes del uso del contenido, por ejemplo el acceso de un contenido requerirá un pago) a lo largo de un ciclo de vida entero de un contenido. Lo que implementará tener un licenciamiento confiable que contendrá la especificación de derechos seguros o en otras palabras una descripción de permisos para el uso adecuado del contenido y la ejecución y el cumplimiento de éstos, en el cuál se utilizaran algoritmos confiables para el cifrado de los contenidos digitales.



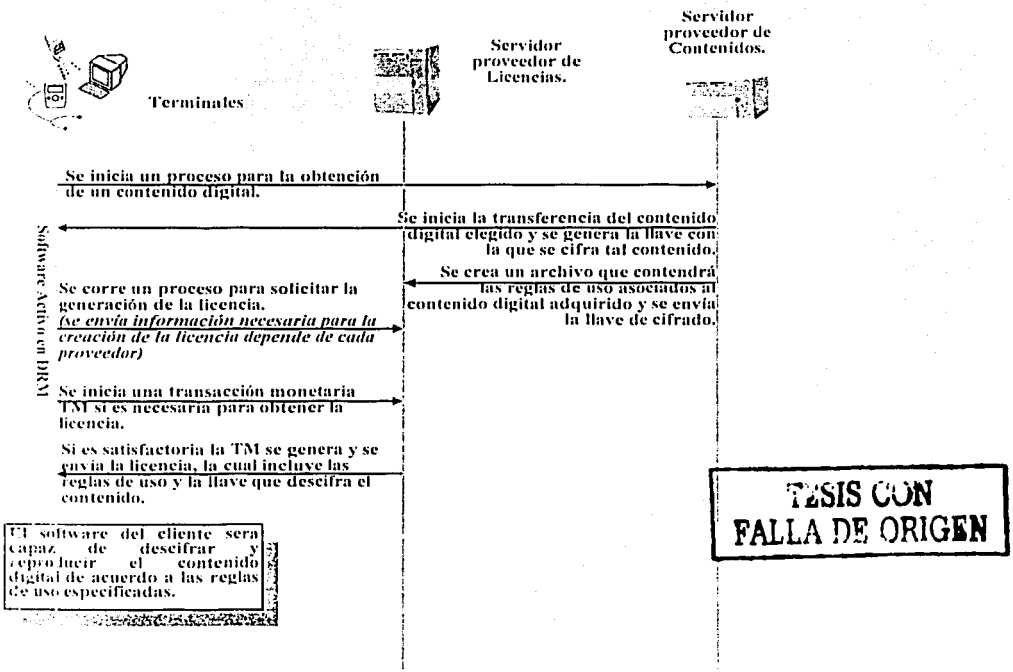
Cadena de valores de los Contenidos Digitales

Una solución DRM deberá manejar los aspectos mencionados anteriormente en la cadena de valores de los contenidos para un ciclo tradicional de vida de un contenido.

Un sistema DRM por lo general tiene cuatro componentes principales:

- Un Servidor de Contenido Digital.
- Una red de distribución de contenidos digitales y sus derechos asociados (Operadora de Comunicaciones OpCo)
- Un servidor expendedor de licencias.
- Un software que será capaz de reproducir el contenido en el dispositivo del usuario.

Conceptualmente un Sistema DRM puede esquematizarse de la siguiente manera no olvidando que existe una red de distribución entre los nodos.



Arquitectura base de un Sistema DRM

El esquema anterior es solamente la base de una arquitectura DRM, cada proveedor aporta soluciones propietarias que toman como base el esquema anterior, lo importante de esta arquitectura base es tener presente de una forma conceptual que un sistema para la protección de contenidos digitales puede ser configurado acorde al esquema anterior , la secuencia de los eventos, la configuración de los nodos, y las interfaces que deberán interactuar, así como los

protocolos de comunicación, serán vitales para la implementación de un Sistema DRM conforme a los requerimientos, y modelos de negocio que se implementarán de acuerdo a las necesidades.

En el capítulo 4, se analizaron las herramientas utilizadas para la protección de contenidos digitales las cuales son técnicas de cifrado propuestas en sistemas DRM; se considera una parte esencial el algoritmo que se escogerá para el cifrado de los contenidos y la recuperación de la información original para su posterior reproducción.

En este capítulo se estudio el concepto de criptografía simétrica la cuál es uno de los conceptos más utilizados en Sistemas DRM, se analizo el Algoritmo DES el cuál es un algoritmo que puede verse muy complejo, aunque realmente es un algoritmo de sustitución. Lo que hace es encadenar varios bloques de cifrado, sirviendo la salida de cada uno como clave de cifrado para el siguiente y así la primera palabra del mensaje es cifrada con el primer bloque y el resultado cifrado obtenido se utiliza como clave para cifrar la segunda palabra del mensaje y así sucesivamente.

Los principales inconvenientes que presenta el algoritmo DES son:

- Con la gran potencia de cálculo actual y venidera de las computadoras se creé que se puede violar el algoritmo, aunque eso sí, en un plazo de tiempo que no resultó peligroso para la información cifrada.

Entre sus ventajas cabe citar:

- Es el sistema más extendido del mundo, el que más máquinas usan, el más barato y el más probado.
- Es muy rápido y fácil de implementar.
- Desde su aparición nunca ha sido roto con un sistema práctico.

También se estudio la criptografía asimétrica o de llave pública, en donde se analizo el algoritmo RSA en el cuál si se elige p y q (números primos) muy grandes por ejemplo de 256 bits de longitud es muy difícil deducir matemáticamente la llave de descifrado.

Con una firma Digital y un hash potente se comprobará la autenticidad y la integridad del mensaje cifrado, se emplea este algoritmo para el cifrado de las licencias, ya que nos garantiza que el contenido del mensaje no habrá podido sufrir modificación alguna durante su trayecto hasta que lo obtiene el destinatario.

Las técnicas de Marca de Agua son utilizadas para verificación de la autentificación (tanto del distribuidor o propietario legal, como de que el original no ha sido falsificado) de los

contenidos, tambien nos ayudan al seguimiento de copias no autorizadas, ya que permiten la identificación del autor, propietario distribuidor y/o consumidor autorizado de un contenido digital, la marca de agua, permanece en el contenido en su forma original y no facilita al usuario de poder escuchar, ver, examinar, o manipular el contenido, simplemente ayuda a la autentificación del contenido. Las marcas de agua a diferencia de la encriptación es una herramienta no muy usada, se recurre más a las tecnicas de cifrado, aunque la fortaleza de las marcas de agua radica en:

- Suponiendo que el atacante sepa como la marca de agua fue embebida en el contenido solo el dueño de los derechos de uso, debe saber como detectar o como remover su marca de agua de su contenido.

En el capítulo 5 se describe una Solución DRM-Lite para redes móviles de Tercera Generación.

Una característica importante de los contenidos digitales es el costo de la creación y distribución así como el tamaño del mismo, es decir la cantidad de bits que se utilizaron para la digitalización del mismo, ya que en Internet se permite transmitir cualquier tamaño de contenidos. Se han estructurado dos clasificaciones para la protección de los contenidos digitales, en función del costo de distribución, del costo de contenido y del peso de los contenidos en función de la capacidad de almacenaje en los dispositivos del usuario:

- DRM-Rich
- DRM-Lite.

Sin embargo surge una nueva necesidad proteger el surgimiento de formatos de multimedia-móvil llamados *new media* como la mensajería multimedia, que explotan nuevos formatos de contenidos como son tonos de timbrado, salvapantallas, aplicaciones desarrollados en Java; es entonces como DRM-Lite emerge como una solución para la prevención del uso indebido de contenidos digitales que surgirán con la telefonía móvil de Tercera Generación, este es un sistema basado en la experiencia de la protección de la propiedad intelectual de contenidos con un valor alto dentro de los cuales están las películas, libros electrónicos, videos musicales, etc. distribuidos por Internet con accesos de tipo fijo, a esta solución desde el punto de vista inalámbrico se le ha llamado DRM-Rich.

Debido a las capacidades limitadas del equipo de usuario (relacionado a la capacidad de almacenaje), una solución adecuada para la protección de contenidos digitales es la tecnología de DRM-LITE para redes-originales adaptadas a multimedia de entretenimiento dentro de una estructura de entrega de M-Services.

Los servicios de DRM-Lite deberán ser capaces de:

1. Administrar diferentes tipos de contenidos como también, diferentes valores de los contenidos, por ejemplo una forma de DRM ha sido implementada para la distribución y consumo de tonos de timbrado e iconos en este caso hay dos componentes para el sistema DRM; una es controlar el acceso a los tonos de timbrado e iconos restringiendo la distribución de los tonos de timbrado. Los subscriptores tienen usualmente que realizar una transacción financiera para obtener el acceso a un único tono de timbrado y las distribuciones será restringida ya que no habrá una funcionabilidad de distribuir los tonos de timbrado e iconos una vez almacenado en el dispositivo móvil.
2. Distribuir una gran variedad de contenidos digitales que tendrán diferentes valores y derechos asociados. Se cree que los servicios DRM creados deberán proveer una administración y protección persistente para las reglas de negocio impuestas por los proveedores de contenidos como por ejemplo ver un cierto número de veces, reproducir el contenido por un determinado tiempo, etc.

Los pasos de una solución DRM Lite se muestran a continuación:

1. El contenido se transmite entre el autor/dueño/creador del contenido y una red fiable sobre redes seguras intermedias protegidas por ejemplo con SSL, TLS o IPSec.
2. La arquitectura de sistema DRM proporciona la capacidad de restringir la transmisión (descarga) de medios/contenidos protegidos a un equipo de usuario, es decir siempre se verifica en el registro del Perfil de Agente de Usuario del dispositivo (que puede estar en una base de datos de la OpCo) si este soporta DRM.
3. Se entrega el contenido al equipo de un usuario final dentro de una red fiable usando WTLS. Una vez entregado el contenido este no puede ser transferido fuera de dicha red, por ejemplo dentro del contexto de MMS, el manejo de la estructura de los derechos de uso esta definida dentro del cuerpo del mensaje con el archivo RIF como un segundo objeto en la estructura de MIME.
4. El Agente de Usuario DRM que tiene un equipo de usuario que tiene las siguientes características:

4.1 No permite la distribución de contenidos vía conectividad local por ejemplo: Bluetooth, USB, IrDA, etc.

4.2 Provee 'seguridad de almacenaje' del objeto de multimedia y derechos asociados.

4.3 Cuando el contenido es suprimido (borrado) los derechos asociados son suprimidos (borrados) con cualesquier referencia.

5. Los objetos con derechos de uso asociados son indicados dentro del HTTP multipart/relacionado o en el WSP vnd.wap.multipart.mixed en cabecera MIME.
6. El lenguaje para la definición de derechos REI será Open Digital Rights Language (ODRL)

   6.1 Específicamente, la RIF basada en ODRL soportará: UID, Display, Play, Execute, Copy, Narrow.

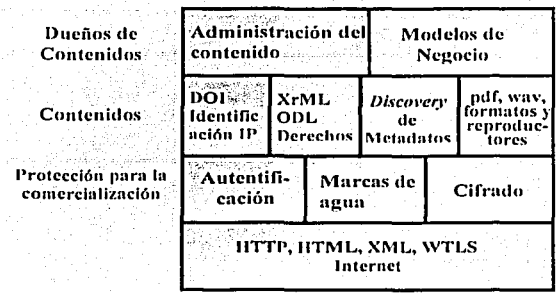
Esta solución proporciona a los creadores/dueños de los contenidos de multimedia asegurar que sus contenidos no serán re-transmitidos a otros usuarios dentro de la red móvil que tenga implementada un Sistema DRM, ni tampoco por sistemas propios del terminal, o por terceros; asegurándoles también el buen uso de los mismos y obtener las recompensas económicas de su obra.

En el capitulo 6 se vieron dos temas importantes la estandarización y soluciones de algunos proveedores en Sistemas DRM

La estandarización juega un papel muy importante, asegura la compatibilidad, la integración y facilita la adopción de cada uno de los integrantes de la cadena de valores y en nuestro caso se hablaría de la cadena de valor de los contenidos.

Sin embargo los trabajos propietarios son típicos en los productos que están surgiendo en el mercado, los sistemas de DRM necesitan abarcar a los estándares que están emergiendo para asegurar a su contenido dentro de los cuales se encuentran los estándares de encriptación empleando algoritmos AES, DES, RSA, para la definición de derechos y de las reglas de uso se utilizan lenguajes para especificar los derechos los cuales son ODRL, XrML, y XMCL para la identificación del contenido se utiliza el DOI y para la descripción de lo que contiene un archivo encriptado se utilizan los metadatos.

Se propone la siguiente jerarquía para los estándares de DRM:



Jerarquía propuesta para un Sistema DRM

En la figura anterior se esquematiza la configuración de varias capas relacionadas con la estandarización DRM y como se relacionan con los estándares básicos de Internet.

Se analizaron dos soluciones propietarias de proveedores de Plataformas DRM.

La primera una solución de Microsoft una plataforma para accesos de tipo fijo a Internet llamada Administrador de derechos de Windows Media (Microsoft ® Windows Media™ Rigths Manager).

En la cuál el proceso de distribución protegida de archivos Multimedia de Windows con WMRM es esquematizado dentro de cinco áreas:

- Creación de contenido digital y posterior codificación a un formato de Windows Media.
- Empaquetado de archivos basados en Windows Media.
- Distribución de los archivos empaquetados a los consumidores
- Generación y emisión de licencias
- Reproducción de archivos empacados y administración de licencias.

Es una solución bastante robusta en la generación de llaves de cifrado de los contenidos digitales y de las licencias.

- Las licencias son emitidas independientemente de los archivos de Multimedia de Windows, proporcionando una máxima flexibilidad y así mismo permitiendo una amplia distribución del contenido.

- La fortaleza de esta solución radica en el esquema de cifrado que utilizan, se generan una llave de cifrado con ID de la llave + semilla de la llave de la licencia con la cual se cifra el contenido digital, y la cabecera del paquete se firma digitalmente para asegurar que cuando el paquete sea recibido se compruebe la integridad.
- Usa algoritmos de cifrado muy fuertes y hace comprobaciones de integridad en tiempo de ejecución. El proceso es rápido más de 540 KB por segundo. Todos los paquetes de carga útil son cifrados individualmente pero el aumento es mínimo. Para firmas digitales utiliza RSA, DSS, *Elliptic Curve*, y para el cifrado de contenidos digitales algoritmos simétricos como: RC4, DES.

La segunda es una solución DRM desarrollada por el proveedor Nokia para contenidos digitales que son distribuidos en redes con accesos a Internet de Tipo Inalámbrico. Esta solución aún no esta implementada por completo, se esta desarrollando el software del teléfono móvil que será capaz de interpretar el *vaucher* que contiene los derechos, se esta aún trabajando con los fabricantes de los dispositivos móviles.

Esta solución presenta las siguientes características relevantes:

- El contenido y los derechos están separados.
- El uso de las reglas está expresado en un *voucher* (vale), usando un Lenguaje de Expresión de Reglas.
- El uso de reglas está descrito en el *voucher*, el cual se implementará por el *middleware* del teléfono móvil.
- En esta solución se propone un nodo nuevo, El Agente DRM o *DRM broker* es un host para la recolección del pago o de regalías por la adquisición de los contenidos digitales, el cuál podría ser también el operador. El broker es efectivamente un "Rigths-clearing feature" de una solución de pago móvil con interfaces a sistemas de pagos.
- El punto fuerte de esta solución es proponer la compra de un *voucher*, el cuál se entregara cuando haya sido pagado, si no se obtiene tal *voucher*, el contenido digital no podrá ser reproducido.

El analizar las soluciones propuestas por estos dos proveedores, ayuda a entender mejor el concepto DRM, las cuáles están basadas en el esquema general del Sistemas DRM, cada proveedor provee una solución propietaria, añadiendo nuevos nodos, o proponiendo diversas formas de cifrado.

7.1. Hacía donde vamos.

Un sistema DRM es una solución para contrarrestar el uso indebido por parte de los usuarios de cualquier clase de Contenido Digital, desde fotografías, canciones, tonos de timbrado hasta entrevistas de cualquier índole; siempre que estos tengan un derecho de autor asociado.
Finalmente se señala que los Sistemas DRM en un futuro penetraran fuertemente en todas aquellas Industrias que deseen distribuir y vender sus contenidos digitales a través de cualquier tipo de red y que deseen obtener regalías por la compra y uso adecuado de sus bienes digitales. Se piensa que próximamente podría convertirse en una necesidad y que tal vez se inicie como algo permanente.
Un sistema DRM no solo será utilizado como hasta ahora en PC's si no tendrá una rápida movilización hacía otros dispositivos como teléfonos móviles, ya que la implementación de una red de comunicaciones móviles de Tercera Generación creara un nuevo canal para el acceso, la distribución y las ventas de Contenidos Digitales protegidos.
Un sistema DRM es una propuesta novedosa, hoy en día no hay mucha literatura, técnicas o soluciones de proveedores relacionadas con el tema, sin embargo las bases están cimentadas, las próximas líneas de desarrollo se enfocaran en la optimización del proceso para la generación, de algoritmos de cifrado y de la obtención de las mismos para el descifrado y reproducción de los contenidos digitales, marcas de agua robustas, así como también la elección del estándar más adecuado con el cuál se definirán las reglas de autor asociadas al contenido digital protegido. Es importante hacer notar que estas líneas estarán orientadas conforme a los nuevos modelos de negocio que surgirán, en los cuales se definirán de acuerdo a los requerimientos de las tecnologías involucradas.

Referencias.

[1] Hill Rosenblatt, Bill Trippe and Stephen Mooney
Digital Rights Management
Ed. M&T Books 2002

[2] C.C-Chang, K.F-Hwang, M.S-Hwang
Robust Authentication schema for protecting copyrights of image and graphic
IEE Proc Vis. Image Signal Process, Vol 149, No. 1 February 2002.

[3] Duhl, Joshua
The DRM Landscape: Technologies, Vendors and Markets. (white Paper)
IDC Report #24891, Jun 2001.

[4] Gervais, Daniel J.
Electronic Rights Management and Digital Identifier Systems.
Journal of Electronic Publising.
Volume 4 Number 3, Mar 1997

[5] Samtani, Rajan
Following the Money: Managing Intellectual Property in the Digital Age.

[6] Vijay K. Grang
Wireless Network Evolution: 2G to 3G.
Ed. Prentice Hall 2002.

[7] Steven Atkinson
Multi-Media Content Services (White Paper)
Version 0.11 Draft, Vodafone.

[8] Duhl, Joshua and Susan Kevorkian
Understanding DRM Systems (white Paper)
IDC Report, Jun 2001.

[9] Carl Gunter, Stephen Weeks, and Andrew Wright
Models and Languages for Digital Rights (white Paper)
Technical reports STAR-TR-01-04, march 2001.

[10] Susana Hornillo Mellado.
"Apuntes de Digital Watermarking "
Tratamiento Digital de Señales en Comunicaciones.
Universidad de Valencia, España.

[11] http://www.ietf.org

[12] http://www.3gpp.org

[13] http://www.eriesson.com

[14] http://www.cellular.co.za/technologies/3g/3g.htm

[15] http://msdn.microsoft.com/msdnmag/issues/01/12/DRM/print.asp

[16] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmform/htm/digitalrightsmanagementfeatures.asp

[17] http://mae.mae.eie.uva.es/~eemm02/printer.pdf

[18] http://www.xrml.org.

[19] http://www.qualcom.com

[20] http://www.oasis-open.org/cover/ericksonRT19990624.pdf

[21] http://odrl.net/ODRL-08.pdf

[22] http://www.iprsystems.com/html/rights_management.html

[23] http://home.een.ab.ca/%7Ejsavard/crypto/jscrypt.htm