J. A. Onieva, J. Lopez, R. Roman, and J. Zhou, "Extension de una plataforma DRM basada en OMA con servicios de No Repudio", *IX Reunion Española sobre Criptologia y Seguridad de la Informacion (RECSI06)*, pp. 129-141, 2006.
NICS Lab. Publications: https://www.nics.uma.es/publications

Extensión de una plataforma DRM basada en OMA con servicios de No Repudio

Jose A. Onieva[1], Javier Lopez[1], Rodrigo Román[1], and Jianying Zhou[2]

[1] Departamento de Lenguajes y Ciencias de la Computación, Universidad de Málaga, 29071 - Malaga, España
{onieva,jlm,roman}@lcc.uma.es
[2] Institute for Infocomm Research
21 Heng Mui Keng Terrace, Singapore 119613
jyzhou@i2r.a-star.edu.sg

Resumen Digital Rights Management (DRM) es un término general para cualesquiera de las soluciones que permite a un vendedor de contenido en forma electrónica controlar el material y restringir su uso de distintas maneras. Estas soluciones son posibles, por un lado gracias a técnicas de la Seguridad de la Información, principalmente cifrado de datos, y por otro a la distribución, de manera independiente, de contenido y derechos digitales. Esto permite que los consumidores puedan acceder libremente al contenido, pero sólo aquellos que adquieran el derecho digital apropiado (RO) podrán procesarlo. Como servicio de seguridad considerado en diversas capas del marco de seguridad definido por la recomendación ITU X.805, casi todas las aplicaciones necesitan considerar la propiedad de no repudio en las etapas iniciales de su diseño. Desafortunadamente, esto no ha sido así en general, y más concretamente en especificaciones DRM; debido a consideraciones en la práctica y al tipo de contenido a distribuir. Analizamos este servicio para un marco de DRM y proporcionamos una solución que permita que la adquisición de *derechos digitales* sea un operación que no pueda repudiarse.

Keywords - *digital rights management, no repudio, comercio electrónico seguro, aplicaciones móviles.*

1. Introducción

La industria tradicional de contenido multimedia ha utilizado tecnologías clásicas para la distribución y consumo de este tipo de contenidos. No obstante, con el advenimiento de los formatos multimedia digitales y el uso de redes de telecomunicación, la producción y distribución de contenido es más fácil, cómoda y rápida que nunca. Sin embargo, al mismo tiempo, el contenido digital multimedia precisa de una mayor protección contra robo, copias ilegales, etc., y se ha convertido en la mayor batalla que en la actualidad las empresas de contenidos digitales están librando. Esta necesidad al aumento de la protección es conducida por dos tendencias ilícitas: la primera, es la piratería y hurto a gran escala

de los derechos de autor y propiedad de la información; y la segunda, consiste en que cada vez más "información sensible", como por ejemplo documentos financieros, expedientes médicos y contratos, está disponible en forma digital y se debe almacenar, compartir, o distribuir con seguridad en y entre organizaciones.

Éste es precisamente el lugar en el cual las tecnologías DRM nos ofrecen una solución. Técnicamente, DRM se define como un conjunto de tecnologías y sistemas que pueden soportar el ciclo vital entero del contenido (creación, manipulación, distribución y consumo) previniendo copias ilegales, tasas y gastos por copia, permitiendo el procesamiento automático de pagos, monitorizando la distribución de contenido, y protegiendo los derechos y el beneficio de cada entidad.

En estos sistemas, el contenido y los derechos digitales se distribuyen de manera separada. Esta técnica simplifica la transferencia de contenido así como su administración. No hay restricción de contenido y por lo tanto cualquier usuario puede descargarlo. Pero, por supuesto, para poder consumir o procesar dicho contenido, un usuario necesita tener acceso (comprar) al *derecho digital correspondiente* (RO). Podemos distinguir dos métodos principales para la distribución y administración de estos derechos digitales:

Centralizado: Un usuario necesita tener acceso a un servicio central cada vez que desee procesar el contenido. Es muy eficaz contra usuarios malévolos, pero presenta deficiencias a la hora de gestionar fallos (involuntarios o no) del servicio central. Por otra parte, esta solución sufre de problemas del escalabilidad.

Distribuido: Un usuario almacena sus derechos digitales y hace uso de estos cuando lo necesite. Supera las desventajas existentes de los sistemas centralizados pero, sin embargo, para evitar el uso ilegal de derechos, se necesita un hardware especial resistente a manipulaciones o *Dispositivo Personal Confiable* (TPD) que maneja localmente las derechos digitales de manera certificada y resistente a manipulaciones.

Con el advenimiento de las redes celulares, el método distribuido permite la convergencia entre las necesidades del usuario y la industria. Combinando soluciones de DRM con las redes móviles, los usuarios pueden tener acceso a los derechos digitales usando su dispositivo móvil como TPD. Los operadores de telecomunicaciones pueden proporcionar soporte a los usuarios para tener acceso a estos derechos digitales, así como certificar la administración segura de ellos en sus dispositivos (véase la Figura 1).

Hemos modificado una plataforma basada en la especificación 2.0 OMA DRM [11] (que se ha convertido en un estándar aprobado por el *Open Mobile Alliance*) para la administración distribuida de derechos digitales. El esquema modificado propuesto en el proyecto europeo UbiSEC[3] permitirá un marco más seguro para el pago por la adquisición digital de derechos por parte del consumidor, considerando propiedades importantes como el anonimato y la eficiencia (véase la Figura 2).

[3] Ubiquitous Networks with a Secure Provision of Services, Access, and Content Delivery (FP6-2002-IST-1-506926)

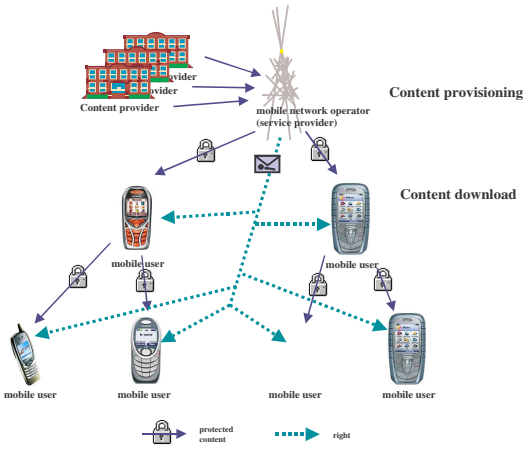

Figura 1. Distribución de contenido

La distribución del RO al usuario a través de un Operador de Telefonía Móvil (MNO) se trata de un paso final importante en la distribución justa de contenido digital (véase la Figura 3). La compra anónima de derechos digitales se hace posible, ya que el Proveedor de contenido y el *Emisor de Derechos* (RI) no requieren datos personales de los consumidores. La facturación del consumidor se realiza con el MNO a el cual se suscribe al cliente. Se genera evidencia digital, de forma que, si algún conflicto se presenta entre las entidades participantes, éstas podrán demostrar su participación en el escenario de DRM. Aunque esta solución se apoye fuertemente en terceras partes confiables (MNO y RI), la propiedad de *no repudio* en la distribución de contenido digital y derechos digitales tiene que ser considerada, minimizando al mismo tiempo el impacto en todas las características anteriormente mencionadas.

Considerando al usuario como el cliente que recibe el contenido y los derechos digitales para poder consumir tal contenido, no repudio es un servicio valioso para el cliente en la última fase en que tiene que acceder al Emisor de Derechos (a través del operador de red móvil) para conseguir el RO en intercambio por el pago. (El MNO cargará al usuario el valor del RO en su factura mensual.)

Incluso aunque los MNO y los RI son consideradas como entidades confiables, puede haber varias dificultades en el proceso (e.g., un fallo de la red o una pérdida de datos) que puede terminar en conflictos entre las entidades participantes. Algunas de estas posibles disputas podrían ser las siguientes.

- El MNO cobra al usuario por un RO que éste no compró o recibió. (Otra posibilidad es que la cantidad de dinero cargada en la cuenta del usuario no coincida con la acordada cuando se realizaba la compra de los derechos digitales)
- El usuario recibe un RO corrupto cuando ya ha pagado por él.

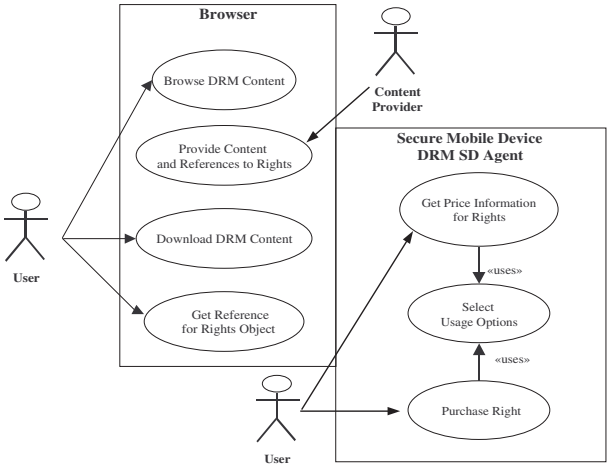

Figura 2. DRM

- El usuario niega haber enviado una petición (RORequest) para adquirir un RO.
- El MNO niega haber recibido una petición del usuario.
- Disputas similares que puedan surgir entre el MNO y el RI.

De esta lista, y según la definición de los servicios de no repudio dados por la ITU, los servicios de no repudio de origen y de recepción tienen que ser proporcionados entre el usuario y el MNO así como entre el MNO y el RI, estableciendo así un canal lógico de no repudio entre usuario y el RI.

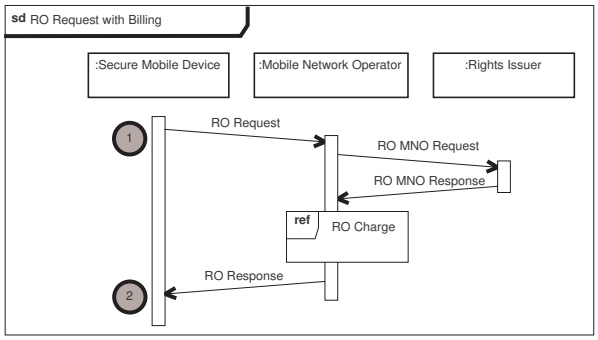

Figura 3. Adquisición del RO

El resto de este artículo se organiza de la siguiente forma. En la Sección 2 introducimos el trabajo relacionado que conocemos. En la Sección 3 describimos la especificación y el modo de funcionamiento de nuestro protocolo de no repudio, así como el proceso de resolución de disputas asociado. En la Sección 4 proporcionamos y discutimos algunas propiedades que surgen de la fase de implementación. Concluimos este artículo en la Sección 5.

2. Trabajos Relacionados

No Repudio es un requisito muy importante en todas las transacciones electrónicas [12]. En nuestro caso, no debe ser posible que un Emisor de Derechos demande que él envió el RO cuando no lo hizo. De la misma manera, no debe ser posible que un usuario niegue de manera fraudulenta el haber recibido el RO. Se debe pues, almacenar evidencia para resolver estos conflictos entre las entidades que participan en un escenario DRM. La firma digital es el principal modo de evidencia criptográfica, que liga un mensaje a su autor al mismo tiempo que mantiene la integridad del mensaje.

Equitatividad ("Fairness") es también una propiedad deseable en las transacciones electrónicas. Se han desarrollado un buen número de soluciones para no repudio equitativo [8]. Algunas de ellas usan una *Tercera Parte Confiable* (TTP) que juega el papel de un intermediario confiable entre las entidades participantes. La desventaja principal de esta solución es el embotellamiento de la comunicación que puede crearse en la comunicación con la TTP. No obstante, Zhou y Gollmann presentaron un protocolo [13] en el que la TTP interviene durante cada ejecución como un "notario ligero" más que como intermediario. Otras soluciones utilizan una TTP off-line, asumiendo que las entidades no tienen ninguna intención maliciosa de forma que la TTP no necesita intervenir a menos que haya un error en la ejecución del protocolo. Esto se denomina como solución optimista. Hay también soluciones que eliminan la participación de una TTP, pero están basadas en un requisito demasiado difícil de cumplir: todos los participantes deben tener la misma capacidad de cómputo. Por consiguiente, en protocolos típicos de no repudio, encontramos tres tipos principales de entidades: emisores u origen (O), recipientes (R), y TTPs.

Existen varias iniciativas con respecto al no repudio multiparte [6,9,7,10]. Todas ellas se tratan de estudios teóricos. Usando esos elementos básicos de construcción que aparecen en distintos estudios, hemos diseñado un protocolo que se integra en nuestra plataforma de DRM. Utiliza un intermediario y permite intercambio justo de evidencia en la fase de adquisición del RO[4].

[4] Aunque las peticiones y las respuestas utilizadas en OMA DRM son firmas XML, éstas no aseguran el intercambio justo de contenidos y mensajes, por lo que no proporciona un servicio completo de no repudio.

3. Protocolo

Es muy conveniente en una transacción electrónica recoger, verificar y almacenar evidencias, pero esto puede ser operacionalmente costoso para las entidades que participan. Por lo tanto, las entidades *intermediarias* son necesarias en dichas aplicaciones para ayudar a las entidades finales a realizar sus intercambios dentro del protocolo. Además, estas entidades pueden actuar como enlaces comerciales, aumentando el mercado y las oportunidades no solamente para los clientes sino también para los comerciantes. Está claro que esta filosofía se integra intuitivamente con las soluciones móviles de DRM en las cuales el operador de red móvil sirve como entidad intermediaria y los usuarios tienen acceso directo a él, poniendo de forma implícita cierto grado de confianza en éste.

Como hemos visto, el MNO desempeña un papel crítico en este escenario, así que es importante analizar su comportamiento. Ya que el MNO tiene interés (facturación) en una transacción del tipo que venimos describiendo, estará dispuesto a que la transacción electrónica tenga éxito. Pero, ocasionalmente, el MNO puede confabularse con otra entidad (externa o interna) y, por ejemplo, ocultar cierta evidencia digital. Por lo tanto, asumimos que la confianza en el MNO no es completa. Presumimos que el MNO no va a ocultar el mensaje inicial RORequest del consumidor al RI. Debido a que el MNO se comunica directamente con el RI, podría ayudar al cliente en el protocolo de no repudio.

3.1. Descripción del protocolo

La notación utilizada en el protocolo puede encontrarse en la Tabla 1:

$A \rightarrow B : X$	la entidad A envía el mensaje X a la entidad B
$A \leftrightarrow B : X$	A puede acceder al mensaje X almacenado por B
X, Y	concatenación de los mensajes X e Y
$S_P(X)$	firma digital del usuario P sobre el mensaje X
$h(X)$	función hash sobre una entrada X

Cuadro 1. Notación General

Una notación más detallada de los elementos del protocolo es la que sigue:

- $l = h(U, RI, MNO, TTP, t, RORequest)$: identificación del mensaje $RORequest$
- t: una fecha límite elegida por el usuario U, antes de la cual la TTP debe publicar cierta información
- $EOO = S_U(MNO, RI, TTP, l, t, PriceInfo, RORequest)$: evidencia de origen del envío de $RORequest$, el cual ha sido generado por U
- $EOO_{MNO} = S_{MNO}(RI, TTP, l, t, ROMNORequest)$: evidencia de origen del envío de $RORequest$ desde el MNO hacia el RI
- $EOR = S_{RI}(MNO, l, t, ROMNOResponse)$: evidencia de recibo de $ROMNORequest$, el cual ha sido generado por RI

- $EOR_{MNO} = S_{MNO}(U, RI, TTP, l, t, PriceInfo,$
  $ROResponse)$: evidencia de recibo de $RORequest$ enviado desde el MNO hacia U, y al mismo tiempo, evidencia de origen de $ROResponse$
- $Con = S_{TTP}(MNO, RI, l, t, PriceInfo,$
  $ROResponse)$: evidencia de confirmación generada por la TTP

El protocolo se describe a continuación. Se asume la inclusión de un flag dentro de cada mensaje (y de cada información firmada) que indique su propósito.

1. $U \rightarrow MNO \quad : MNO, RI, TTP, l, t,$
   $PriceInfo, RORequest, EOO$
2. $MNO \rightarrow RI : RI, TTP, l, t,$
   $ROMNORequest, EOO_{MNO}$
3. $RI \rightarrow MNO : MNO, l,$
   $ROMNOResponse, EOR$
4. $MNO \rightarrow U, TTP : U, RI, l, t, RORequest,$
   $PriceInfo, ROResponse, EOR_{MNO}$
5. $All \leftrightarrow TTP : MNO, RI, l, PriceInfo,$
   $ROResponse, Con$

El protocolo funciona de la siguiente forma:

1. U envía al MNO la evidencia de origen correspondiente a su $RORequest$ y al $PriceInfo$ obtenido tras buscar los derechos correspondientes. Ninguno de los participantes obtiene una ventaja en caso de que el protocolo se detenga aquí, por lo que el protocolo se mantiene justo.
2. MNO distribuye la información recibida de U (quizás después de una negociación con el RI y después de haber preparado $ROMNORequest$ utilizando el $RORequest$ del usuario) y envía también a RI evidencia de su participación en la transacción. De nuevo, se mantiene la equitatividad en caso de que el protocolo sea detenido.
3. RI responde con la evidencia de recibo de $RORequest$, junto con el $ROMNOResponse$. Se asume que existe un canal seguro entre el MNO y el RI. El protocolo se mantiene justo en este momento, ya que ninguna de las entidades ha obtenido lo que quería (U necesita $ROResponse$, mientras que RI y MNO necesitan la evidencia de que la transacción se ha llevado a cabo). Ha de puntualizarse que $RORequest$ se identifica de forma única mediante la etiqueta l.
4. MNO envía al U el RO ($ROResponse$) junto con la evidencia de haber recibido $RORequest$, y envía una copia de esa evidencia al TTP. U y TTP comprobarán todas las evidencias recibidas hasta este momento antes de proceder con el siguiente paso. Para U, ésta (EOR_{MNO}) es la única evidencia que recibirá del MNO, y que utilizará en caso de disputas para demostrar la responsabilidad del MNO durante el intercambio. MNO almacenará la evidencia de recibo de RI en su base de datos y U puede obtenerla más tarde si la necesita. MNO no puede justificar que no almacenó esa evidencia de recibo puesto que EOR_{MNO} demostraría lo contrario. Tanto U como TTP comprueban lo siguiente:

- $l = h(U, RI, MNO, TTP, t, RORequest)$
- La información recibida se encuentra firmada por el MNO
- $tiempo\_actual < t$

Si *ROResponse* es el objeto que U esperaba (el cual debe incluir la información sobre su precio), éste no necesita continuar con el protocolo, puesto que ya ha obtenido lo que quería. En caso contrario, p.ej. si *ROResponse* o la información sobre el precio del objeto no se han recibido o estan dañados, U participará en el siguiente paso.

5. TTP publica el mensaje de confirmación. U recoge *ROResponse*, $PriceInfo$ (si no está satisfecho con los resultados del paso anterior) y Con como evidencia del Derecho Digital (RO) que ha comprado. MNO recoge Con como evidencia de que U ha recibido (o ha recogido del TTP) EOR_{MNO} y el RO (junto con su importe correspondiente) emitido por el RI. RI recoge Con como evidencia para probar el origen del RO. Es importante hacer notar que si MNO ejecuta el paso 4 con $tiempo\_actual > t$, no obtendrá ninguna ventaja. Es más, U podria obtener el RO sin tener que pagar por él, ya que TTP no generaría Con.
   Por otro lado, si MNO intenta hacer trampas cambiando la fecha límite, entonces la evidencia Con no coincidirá con el resto de las evidencias. De esta forma, todas las entidades están seguras cuando se sobrepasa la fecha límite t.

Al finalizar el protocolo, cada uno de sus participantes poseerá un conjunto de evidencias que le permitirán resolver las disputas que puedan surgir.

- U recoge EOR_{MNO} y/o Con como evidencias de la participación del MNO.
- MNO recoge EOO, EOR, y Con como evidencia de origen y evidencia de recepción, respectivamente, lo cual le permitirá demostrar su buen comportamiento a lo largo del protocolo.
- RI recoge EOO_{MNO} y Con como evidencia de origen del *ROResponse* enviado por el MNO.

Este protocolo se desarrolla en unicamente cinco pasos, y permite preservar el anonimato del usuario. Es decir, a menos que el usuario decida comunicarse con un RI predeterminado, ninguno de los dos necesita conocer información acerca del otro (p.ej. certificados) para el correcto funcionamiento del protocolo. Esto permite que nuestra infraestructura DRM conserve su propiedad de anonimato, y puede utilizarse en el caso que el MNO pueda elegir entre varios RI (p.ej. dependiendo de la confianza que tenga en cada uno de ellos).

3.2. Resolución de disputas

Dentro de nuestro modelo, las disputas más comunes que pueden surgir se detallan mas adelante. En el caso que las evidencias tengan una fecha de caducidad, toda disputa debería resolverse con la ayuda de un *juez digital* antes de ese momento. Todas las entidades (incluyendo la TTP) sólo almacenan evidencias

durante su vida útil, la cual normalmente no excede de un mes (si las facturas de pagan mensualmente).

Disputas entre el usuario y el MNO

Si el usuario ha pagado por un Derecho digital (RO) y este resulta ser inservible, pero el MNO lo niega, U puede presentar $ROResponse$, $PriceInfo$, EOR_{MNO} y/o Con a un intermediario. Éste comprobará la validez del identificador l, y también comprobará que $(l, PriceInfo, ROResponse)$ está firmado por el MNO en EOR_{MNO} o por el TTP en Con. En este caso, el juez determinará que MNO no envió al usuario un RO válido.

Si el MNO cobra al usuario un RO determinado (incluido dentro del $ROResponse$) pero ese usuario niega haberlo comprado o haberlo recibido, el MNO deberá presentar EOO y Con a un intermediario. Éste comprobará la firma de U en EOO (demostrando que pidió ese RO) y la firma de TTP en Con. En este caso, el intermediario determinará que U obtuvo $ROResponse$ (o pudo recogerlo de la TTP), y por tanto, recibió el RO del MNO. Note that as we will see in next section $RORequest$ and $ROResponse$ are linked.

Disputas entre el RI y el MNO

Si el MNO niega haber enviado el mensaje $RORequest$ (es decir, $ROMNORequest$ una vez transformado por el MNO) al RI, éste puede presentar la evidencia EOO_{MNO} a un juez digital, el cual verificará la firma del MNO incluida en la evidencia. En este caso, determinará que $RORequest$, creado inicialmente por U, fué enviado al RI por el MNO. En otro caso, si RI niega haber recibido el mensaje $RORequest$, el MNO proporcionará la evidencia EOR y juez digital verificará la firma del RI incluida en la evidencia. Si la verificación es correcta, determinará que el MNO envió $RORequest$ al RI.

RI recoge Con para poder demostrar que la transacción con el usuario finalizó. Esto es útil en caso de que el RI cobre al MNO dependiendo del número de derechos digitales que hayan sido distribuidos satisfactoriamente.

4. Diseño e Implementación

En esta sección se muestra brevemente el diseño y la implementación del sistema (ver figura 4). En primer lugar, identificaremos las diferentes operaciones (sean estos procesos o parte de una API) a llevar a cabo, describiendo su funcionamiento en detalle. Solo mostraremos las operaciones más importantes:

U - Teléfono Móvil: Un usuario maneja el teléfono móvil, obteniendo servicios DRM. Las operaciones dentro del teléfono móvil son:

- *(API)* ***ObtenerROResponse***. Entrada: $RORequest$. Salida: $[ROResponse|Error]$. *Operaciones internas*: El teléfono móvil negocia con el MNO (enviando EOO y recibiendo EOR_{MNO}) y con el TTP (recogiendo Con), obteniendo el RO Digital incluido dentro de $ROResponse$ junto con las evidencias de las comunicaciones realizadas. *Operaciones adicionales*: U **debe** comprobar y almacenar EOR_{MNO} y/o Con como evidencia de recibo. *Notas*: U contacta con la TTP si EOR_{MNO} está dañada o se ha perdido.

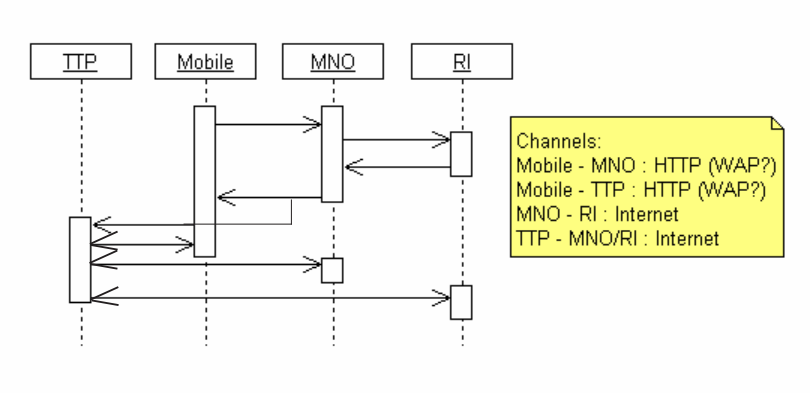

Figura 4. Flujo de las comunicaciones HTTP

MNO - Operador de Telefonía Móvil (*Mobile Network Operator*): Proporciona servicios para la adquisición del RO, contactando con un TSP (Proveedor de servicios, *Third-party Service Provider*) que actua como un RI. Las operaciones son:

- *(Process)* ***ManejarRORequestDeU***. Activado por: *EOO*. Parar: en caso de *Error*.
  Operaciones internas: MNO recibe *EOO* del U. Genera y envía EOO_{MNO} al RI, recibiendo *EOR* de éste. A continuación, crea y envía EOR_{MNO} al U y a la TTP.
  Operaciones adicionales: MNO **debe** verificar y almacenar *EOO* y *EOR*.
  Notas: Este proceso debe tener un interfaz que le permita acceder a recursos globales de la infraestructura del operador, tales como bases de datos de evidencias y sistemas de cobro y facturación.

RI - Emisor de Derechos (*Rights Issuer*): Recibe mensajes *RORequest* de otras entidades, y accede a los objetos DRM para proporcionar un *ROResponse* adecuado a la petición.

- *(Proceso)* ***ManejarRORequestDelMNO***. Activado por: EOO_{MNO}. Parar: en caso de *Error*.
  Operaciones internas: RI recibe EOO_{MNO} del MNO. Se encarga de llamar al objeto DRM *ROResponse* usando *RORequest* como parámetro. Si éste responde con un objeto *ROResponse*, genera y envía *EOR* al MNO. Es decir, el objeto DRM *ROResponse* contiene a *RORequest*.
  Operaciones adicionales: RI **debe** verificar y almacenar EOO_{MNO}.

TTP - Tercera Parte Confiable (*Trusted Third Party*): Recibe las claves de las redes de telefonía móvil, y las distribuye junto con otros tipos de información (evidencias).

- *(Process)* ***RecibirClavedelMNO***. Activado por: EOR_{MNO}. Parar: en caso de *Error*.
  Operaciones internas: El TTP recibe EOR_{MNO} del MNO. Después de comprobar que el mensaje ha sido recibido antes del límite t, genera *Con* y lo almacena para un uso posterior.
  Operaciones adicionales: TTP **debe** almacenar el mensaje *Con* junto con su identificador asociado l. Después, U, MNO, y RI recogerán ese mensaje utilizando para ello el identificador l.

Aunque la TTP sea una entidad distinta e independiente al MNO, es posible utilizar GPRS para contactar con ella en tanto que la conexión HTTP soporte SSL. Esto evitaría que el MNO intentara denegar el servicio cuando el usuario U realiza un acceso a la TTP. No obstante, en nuestro prototipo estamos utilizando una conexión 802.11 (IP), evitando así que el flujo de información al TTP circule a través del MNO.

Como ya hemos mencionado en la sección 2, las firmas digitales son la principal herramienta a utilizar para el manejo de evidencias. Actualmente, generar firmas digitales utilizando dispositivos de recursos limitados (tales como móviles) no es una operación restrictiva. Por ejemplo, en nuestro prototipo, el teléfono móvil (modelo Siemens SX1) es capaz de calcular todas las operaciones criptográficas en 6 segundos.

Para la implementación del sistema del teléfono móvil hemos utilizado J2ME-MIDP 1.0 [3] mientras que para el resto de los componentes (RI, MNO, TTP) hemos utilizado J2SE y Servlets J2EE para la implementación de los servicios HTTP. Las operaciones criptográficas se han realizado (tanto en entornos móviles (J2ME) como en entornos de servidor (J2SE/J2EE)) utilizando la librería *Bouncy Castle Crypto Lightweight Library* [4]. (Existe un estandar para MIDP, JSR 219 [1], aún no disponible al tiempo de la implementación.) Finalmente, para procesar XML en entornos móviles, se ha utilizado la librería kXML (*Lightweight XML library for mobile phones*) [2].

Tanto el protocolo como su implementación serán validados como parte del proceso de validación del proyecto UBISEC. Los criterios de la validación se refieren principalmente al cumplimiento de unos requisitos (omitidos en este artículo), los cuales dependen de casos de uso definidos previamente dentro del proyecto UBISEC. Los resultados de la evaluación serán publicados por el equipo técnico de acuerdo al plan de evaluación general (D4.4, aún sin publicar).

5. Conclusiones

Debido al desarrollo de las tecnologías, es de esperar que la descarga de contenidos será una operación casi sin coste alguno para los usuarios. Para proteger los derechos de la propiedad intelectual, las arquitecturas DRM distribuidas constituyen una buena solución. Es más, estas arquitecturas pueden enriquecerse con la inclusión de servicios de seguridad en fases tempranas de su desarrollo. El no repudio es uno de esos servicios.

En este artículo hemos presentado el diseño de un protocolo de no repudio para una plataforma DRM, que tiene en cuenta a todas las entidades que participan en la adquisición de derechos: los usuarios, las operadoras de telefonía móvil (MNO) y los emisores de derechos (RI). De esta forma, se proporciona a cada uno de ellos las evidencias necesarias para utilizarse en caso de disputas.

La implementación del protocolo se muestra brevemente. Esta diseñado para su integración dentro de una infraestructura DRM móvil que estamos modificando basándonos en el estándar OMA DRM. Nos encontramos aún en una fase de pruebas, y las APIs necesarias aún no han sido desarrolladas más allá de unos prototipos.

Al mismo tiempo estamos considerando un diseño en el que se integre una solución propuesta por Asokan en su tesis [5], en la que se libera a los usuarios de un servicio de no-repudio de la necesidad de realizar firmas digitales (y especialmente interesante para nosotros al emisor a la hora de crear la evidencia de no-repudio de origen). En esta propuesta, Asokan hace uso de un servidor intermediario (que nosotros planeamos integrar en el MNO) capaz de realizar de forma verificable firmas digitales en lugar del usuario. El receptor solo necesita poder verificar la firma (operación que puede hacerse más eficiente si, por ejemplo, en un sistema de criptografía pública como RSA se utiliza un exponente público pequeño). El principal requisito para el emisor (U) es poder manejar cadenas hash, requisito más sencillo de cumplir para un teléfono móvil que la generación de firmas digitales mediante criptografía asimétrica.

Agradecimientos

El trabajo descrito en este artículo está parcialmente financiado por el proyecto europeo del VI Programa Marco (FP6-2002-IST-1-506926) UBISEC. Al mismo tiempo el primer autor recibe financiación de la Consejería de Innovación, Ciencia y Empresa (Junta de Andalucía) bajo el III Plan de Investigación Andaluz. El tercer autor está financiado por el Programa Nacional de Formación de Profesorado Universitario del MEC.

Referencias

1. JSR 219: Foundation Profile 1.1. http://jcp.org/en/jsr/detail?id=219.
2. kXML. http://kxml.sourceforge.net/index.orig.shtml.
3. Mobile Information Device Profile. http://java.sun.com/products/midp/.
4. The Legion of the Bouncy Castle. http://www.bouncycastle.org/.
5. N. Asokan. Fairness in Electronic Commerce. University of Waterloo, Computer Science, 1998.
6. S. Kremer and O. Markowitch. A multi-party non-repudiation protocol. *Proceedings of 2000 International Conference on Information Security*, pages 271–280, Beijing, China, Agosto 2000.
7. S. Kremer and O. Markowitch. Fair multi-party non-repudiation protocols. *International Journal of Information Security*, 1(4):223 – 235, Julio 2003.

8. S. Kremer, O. Markowitch, and J. Zhou. An intensive survey of fair non-repudiation protocols. *Computer Communications*, 25(17):1606–1621, Noviembre 2002.
9. O. Markowitch and S. Kremer. A multi-party optimistic non-repudiation protocol. *Proceedings of 2000 International Conference on Information Security and Cryptology*, LNCS 2015, pages 109–122, Diciembre 2000.
10. J. A. Onieva, J. Zhou, M. Carbonell, and J. Lopez. A multi-party non-repudiation protocol for exchange of different messages. *Proceedings of 2003 International Conference on Information Security*, pages 37–48, Athens, Greece, Mayo 2003.
11. Open Mobile Alliance. *DRM Specification*, 2nd edition, 2006.
12. J. Zhou. *Non-repudiation in electronic commerce*. Computer Security Series, Artech House, 2001.
13. J. Zhou and D. Gollmann. A fair non-repudiation protocol. *Proceedings of 1996 IEEE Symposium on Security and Privacy*, pages 55–61, Oakland, USA, Mayo 1996.