Smart-Shopping: Aplicación de un Protocolo de Firma de Contratos Multi-Two-Party Atómico

Gerard Draper-Gil, Josep-Lluís Ferrer-Gomila, M. Francisca Hinarejos
Universitat de les Illes Balears (UIB), Email: {gerard.draper, jlferrer, xisca.hinarejos}@uib.es

***Resumen*—El avance de Internet y las tecnologías de comunicaciones está disminuyendo cada vez más la distancia entre consumidores y proveedores, hasta el punto que cualquier proveedor que lo desee puede ofrecer sus productos directamente al consumidor final. Esto supone a la vez una ventaja y una desventaja para el consumidor. Por un lado, le permite comparar los precios de distintos proveedores, pero por otra parte la gran cantidad de oferta puede complicar este proceso. Un caso particularmente interesante es la situación en la que el consumidor quiera un producto multi servicio, como los paquetes turísticos, formados por vuelos, hoteles, excursiones, etc.**

En este artículo presentamos una modificación sobre un protocolo multi-two-party atómico, que permite al consumidor automatizar la función búsqueda, negociación y compra (firma de un contrato), manteniendo la equitatividad y atomicidad en la transacción.

***Palabras clave*—Contratación electrónica multi- party, E- Commerce, Smart Shopping**

I. Introducción

Gracias al comercio electrónico, hoy en día consumidores y proveedores están más cerca que nunca. A través de Internet, los consumidores tienen acceso directo a múltiples proveedores, permitiéndoles, entre otras cosas, comparar distintas ofertas y quedarse con la que más les interese. A su vez, los proveedores tienen acceso directo a millones de clientes potenciales.

Esta situación es de especial interés en sectores como el ocio, donde los consumidores adquieren habitualmente productos como los paquetes turísticos, formados por varios servicios: hoteles, vuelos, excursiones, etc. Los consumidores pueden fácilmente comparar el precio ofrecido para un mismo servicio por distintos proveedores (existen incluso webs específicas para estos servicios) y escoger el que más les convenga. Al final, el paquete que compra el consumidor puede estar formado por servicios de diferentes proveedores. El problema aparece en el momento de ejecutar la compra de los servicios: para que el consumidor obtenga el producto que desea, tiene que comprar servicios diferentes de proveedores distintos, por lo tanto, debe comprometerse con todos los proveedores o con ninguno; sino fuera así, su paquete no estaría completo. A este tipo de escenarios se les denomina Multi-two-Party Atómicos (AM2P).

En un escenario Multi-Two-Party (M2P) tenemos N participantes, 1 consumidor C y $(N-1)$ proveedores P_i, agrupados en un conjunto de $(N-1)$ pares $\{C, P_1\}, \{C, P_2\}..., \{C, P_{(N-1)}\}$, que quieren firmar un conjunto de $(N-1)$ contratos $\{M_1, M_2, ..., M_{(N-1)}\}$ dos a dos, es decir, C y P_1 quieren firmar el contrato M_1, C y P_2 el contrato M_2, etc. En este escenario, ni C ni P_i quieren dar su firma sin tener la seguridad que el otro participante enviará la suya. El escenario *Multi-Two-Party Atómico* (AM2P) es un caso restrictivo del Multi-Two-Party en el que C no quiere enviar su firma sin tener la seguridad que recibirá la firma de *todos* los proveedores $\{P_1, ..., P_{(N-1)}\}$, ni P_i quiere enviar la suya si no recibe la correspondiente firma de C sobre el contrato M_i.

Un artículo presentado en la anterior edición de la RECSI [1] presenta el primer protocolo de firma de contratos dirigido a estos escenarios, donde el consumidor debe negociar previamente con todos los proveedores antes de ejecutar el protocolo. Es decir, el objetivo del protocolo es firmar una serie de contratos pre-acordados entre el consumidor y los distintos proveedores. Este proceso puede ser largo y tedioso, y no todos los consumidores tienen el tiempo o los conocimientos para llevarlo a cabo. Para solucionar esta situación, en este artículo presentamos una modificación sobre el protocolo AM2P, que permite fusionar las fases de negociación y firma, facilitando su uso a los consumidores.

Contribución: En este artículo presentamos una propuesta de protocolo para firma digital de contratos para escenarios *Multi-Two-Party Atómicos*, donde la fase de negociación forma parte del proceso de firma. Esta propuesta es una modificación sobre un protocolo presentado en la última RESCI [1], manteniendo los requisitos de seguridad: efectividad, equitatividad, temporalidad, no-repudio, confidencialidad y verificabilidad de la TTP.

Organización: El artículo está organizado de la siguiente manera. La sección II presenta un ejemplo de cómo podría utilizarse el protocolo presentado en este artículo para crear una aplicación de compra inteligente. En la sección III se describen los requisitos de seguridad del protocolo de negociación más firma *Multi-Two-Party Atómico*. En la sección IV se discute brevemente el trabajo previo realizado, y se presenta el protocolo de firma *Multi-Two-Party Atómico* en el cual se basa este artículo. Nuestra propuesta se define en la sección V. En la sección VI analizamos si nuestra propuesta cumple con los requisitos de seguridad. Finalmente, las conclusiones aparecen en la sección VII.

II. Escenario

El protocolo propuesto en [1], permite a los consumidores firmar un conjunto de contratos, cada uno con un proveedor distinto, de manera atómica y equitativa. Si lo llevamos al terreno práctico, para poder ejecutar el protocolo, el consumidor

ISBN: 978-84-9717-323-0

requiere de una aplicación, o bien nativa o bien como servicio. A esta aplicación el consumidor debería facilitarle un conjunto de contratos, que previamente tiene que haber negociado. Esta fase de negociación previa puede suponer un problema. No todos los consumidores tendrán el tiempo o conocimientos necesarios para llevarla a cabo. La modificación que proponemos sobre el protocolo presentado en [1], permitiría a la aplicación del consumidor automatizar las tareas de búsqueda de proveedores, negociación y firma de contratos.

En la figura 1 se muestra un ejemplo de cómo podría utilizarse el protocolo para implementar una aplicación de compras inteligente. El funcionamiento sería el siguiente:

1. El consumidor le indica a la aplicación que quiere comprar un paquete compuesto por un servicio aéreo y un alojamiento (orden de compra). Para cada uno de los servicios le indica las opciones que desea. Por ejemplo, en el caso del servicio aéreo, las fechas del viaje, origen y destino, horarios, etc... Además, el consumidor puede indicar un precio máximo para el paquete completo, sus preferencias en caso de que el producto sea ofrecido por más de un proveedor, incluso podría indicar un tiempo màximo en el que la aplicación debe contestar (inmediatamente, un día, una semana, ...).
2. La aplicación consultará su base de datos de proveedores y recuperará la lista de proveedores que puedan ofrecer los servicios reclamados por el consumidor. Esta base de datos puede ser un servicio preconfigurado en la aplicación, un listado que el propio consumidor haya confeccionado, un servicio externo (por ejemplo UDDI [2]), etc.
3. Una vez se ha generado la lista de proveedores, se inicia el protocolo de negociación + firma con cada uno de ellos. En el caso del ejemplo, se han encontrado 3 proveedores de servicios aéreos y 2 proveedores de servicios de alojamiento.
4. Como resultado, la aplicación de compras le devuelve al consumidor el contrato firmado con cada uno de los proveedores seleccionados (para firmar), en este caso han sido el proveedor P_{V1} de servicios aéreos y el proveedor P_{H1} de servicios de alojamiento.

¿Cómo se introduce la negociación en el proceso de firma?, veamos el caso del ejemplo de la figura 1. La aplicación de compra preparará un contrato para cada uno de los proveedores que ha encontrado en la base de datos: $\{M_{P_{V1}}, M_{P_{V2}}, M_{P_{V3}}, M_{P_{H1}}, M_{P_{H2}}\}$, y lanzará la petición a todos ellos. Supongamos que los proveedores P_{V1} y P_{V2} aceptan la petición y el proveedor P_{V3} la rechaza. En este caso la aplicación de compras deberá escoger entre P_{V1} y P_{V2} para continuar con la ejecución, mientras que al proveedor descartado deberá enviarle un mensaje de rechazo. Los criterios a seguir pueden ser varios, por ejemplo las preferencias del consumidor (puede indicar proveedores favoritos), el tiempo de respuesta, o un valor de reputación. Pero antes de poder contestar al proveedor de servicios aéreos, el consumidor debe recibir al menos una respuesta válida de un proveedor de

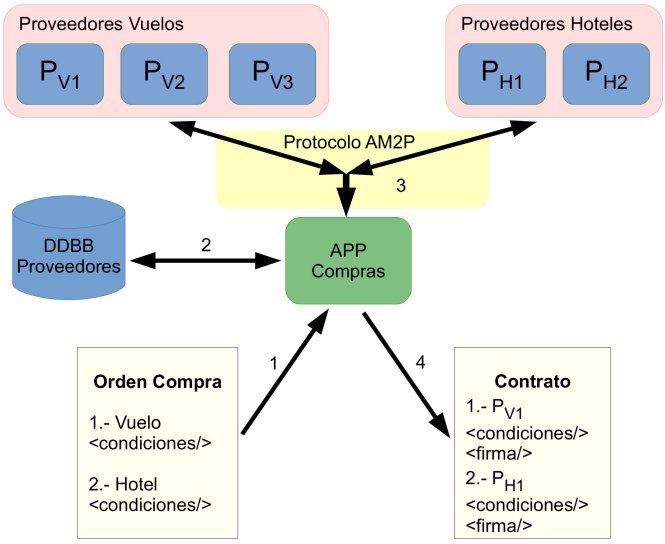

Figura 1. Ejemplo de Aplicación

alojamiento. Una vez el consumidor tiene confirmación de que todos los servicios incluidos en la orden de compra están disponibles, puede continuar con la ejecución del protocolo.

III. Requisitos de Seguridad

Asokan *et al.* [3] y Zhou *et al.* [4] establecen los requisitos mínimos para el intercambio equitativo: efectividad, equitatividad, temporalidad, no-repudio y verificabilidad de la TTP. Aunque de hecho, la verificabilidad de la TTP no es estríctamente necesaria para que un protocolo sea equitativo. Es más, Asokan *et al.* [3] define 2 tipos de equitatividad, débil y fuerte, mientras que Zhou *et al.* [4] define sólo uno, que coincide con la equitatividad fuerte. Otro requisito deseable es la confidencialidad. A continuación detallamos los requisitos para el protocolo equitativo Multi-Two-Party Atómico definido en este artículo:

- **Efectividad.** Si todas las partes involucradas en un protocolo de negociación más firma Multi-Two-Party Atómico se comportan correctamente, el consumidor recibirá la firma de los $(N-1)$ proveedores seleccionados, y estos recibirán la correspondiente firma del consumidor. Además, todos los proveedores que hayan sido descartados recibirán un mensaje de rechazo por parte del consumidor, y éste recibirá el correspondiente reconocimiento por parte del proveedor. En caso de que sea el proveedor quien rechaze la negociación, se lo indicará al consumidor. Todos estos mensajes se intercambiarán sin que intervenga la TTP.
- **Equitatividad Débil Multi-Two-Party Atómica.** Al finalizar una negociación más firma Multi-Two-Party Atómica, el consumidor honesto tendrá la firma de los $(N-1)$ proveedores escogidos, y los proveedores honestos tendrán la correspondiente firma o mensaje de rechazo del consumidor; o todas las partes honestas conseguirán

evidencias suficientes para demostrar, ante un árbitro, que se han comportado correctamente.

- **Temporalidad.** Todos los participantes en una negociación más firma Multi-Two-Party Atómica tienen la seguridad de que la ejecución del protocolo de firma tendrá una duración finita. Una vez finalizada, no se puede degradar el nivel de equitatividad obtenida por los participantes honestos, independientemente del comportamiento del resto de participantes.
- **No-Repudio.** En una negociación más firma Multi-Two-Party Atómica en la que hay involucrados un consumidor y $N-1$ proveedores seleccionados por el consumidor, ni el consumidor ni los proveedores pueden negar haber estado involucrados. En particular, dado un contrato firmado M_i, ni el consumidor C ni el proveedor P_i pueden negar haberlo firmado. Además, ninguno de los proveedores descartados puede negar haber sido rechazado por el consumidor, ni el consumidor en caso de que sea el proveedor quien rechaze una oferta.
- **Confidencialidad.** Sólo los participantes involucrados en una firma, es decir, el consumidor C y el proveedor P_i, pueden conocer el contenido del contrato M_i. Ni siquiera la TTP debe tener acceso al contrato en claro.
- **Verificabilidad de la TTP.** Si la TTP actúa de manera deshonesta, provocando la pérdida de equitatividad de un participante honesto (consumidor o proveedor), este puede probar el comportamiento deshonesto de la TTP frente a un árbitro externo.

IV. Trabajo Previo

Pese a los muchos esfuerzos dedicados al estudio del intercambio equitativo, existen muy pocas propuestas [5], [6] que traten el problema que presentamos en este artículo. De hecho, solo una de ellas [5] prevee una fase de negociación, aunque no está integrada en el protocolo de firma, ya que se trata de una fase previa.

En el protocolo de firma de contratos Multi-Two-Party Atómico presentado en [1], sobre el cual se basa la propuesta presentada en este artículo, se incluye una revisión de las propuestas similares existentes. Como conclusión, a dicha revisión y hasta donde conocemos, ninguna de las referencias que hemos encontrado en la literatura en relación con intercambios Atómicos Multi-Two-Party ([5], [6]) cumple con los requisitos de seguridad necesarios, para nuestro escenario (ver sección III).

A continuación se presenta la notación que se va a utilizar a lo largo del artículo:

- $\mathbf{N}$ Número de participantes en la fase de firma: 1 Consumidor y $N-1$ Proveedores.
- $\mathbf{NP}$ Número de proveedores participantes en la fase de negociación: $NP \geq N-1$.
- $\overline{\mathbf{X_Z}} = \{\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_{(Z)}}\}$ Vector con Z elementos.
- $\overline{\mathbf{RP}}$ *Rejected Providers*, conjunto de proveedores que el consumidor rechazará.
- $\overline{\mathbf{AP}}$ *Accepted Providers*, conjunto de proveedores que el consumidor escogerá para continuar la ejecución del protocolo.
- $\mathbf{C}$ Consumidor.
- $\mathbf{P_i}$ Proveedor i, $1 \leq i \leq NP$.
- $\mathbf{M_i}$ Mensaje (contrato) intercambiado entre el consumidor C y el proveedor P_i.
- **CID** Identificador de Contrato Único (Unique Contract IDentifier).
- $\mathbf{h(M_i)}$ Función de Hash del mensaje M_i.
- $\mathbf{S_j[M_i]} = \mathbf{SK_j[h(M_i)]}$ Firma Digital de j sobre M_i (donde SK_j es la clave privada de j).

El protocolo presentado en este artículo está basado en una propuesta previa para la firma de contratos AM2P [1] con N participantes, 1 consumidor y $N-1$ proveedores. Se trata de un protocolo optimista con arquitectura en paralelo, donde el consumidor contacta con todos los proveedores "a la vez", y espera su respuesta antes de continuar con a ejecución, es decir, el consumidor envía $N-1$ compromisos (COMmitment) al mismo tiempo, y espera a recibir las $N-1$ aceptaciones (ACCeptance) antes de continuar. Si el consumidor deja de recibir una o más aceptaciones, contactará con la TTP. Los compromisos son los mensajes enviados desde el consumidor a los proveedores, y las aceptaciones son los mensajes enviados de los proveedores al consumidor. Los $COM_{(n,i)}$ y $ACC_{(n,i)}$ (n = número de ronda, i = número de proveedor) son las evidencias que el proveedor P_i y el consumidor C deben recibir, respectivamente.

La propuesta de protocolo optimista de firma electrónica de contratos AM2P [1] está dividida en dos sub-protocolos: *intercambio* y *resolución*. Si todas las partes involucradas se comportan correctamente, el sub-protocolo de *intercambio* terminará después de N rondas, se intercambiarán $2N(N-1)$ mensajes y la TTP no intervendrá.

Cada ejecución completa del sub-protocolo de *resolución* está compuesta de N rondas, y cada ronda requiere el intercambio de $N-1$ pares de mensajes {compromiso, aceptación}, lo que hace un total de $2N(N-1)$ mensajes. Las evidencias de firma son las correspondientes a la ronda N ($COM_{(N,i)}$ y $ACC_{(N,i)}$). En cualquier momento, el consumidor y los proveedores pueden ejecutar el sub-protocolo de *resolución* para resolver la ejecución del protocolo. Durante la primera ronda ($n=1$), cualquier participante puede contactar con la TTP y solicitar que se cancele la firma, mientras que si $n>1$, la petición tendrá como objetivo finalizar el protocolo (firmar el contrato).

V. Protocolo

El protocolo presentado en este artículo mantiene la estructura original, una arquitectura en paralelo donde el consumidor y los proveedores intercambian N pares de mensajes {compromiso, aceptación}.

V-A. Sub-Protocolo de Intercambio

En la tabla I podemos ver el flujo de ejecución del protocolo y los mensajes intercambiados. La fase de negociación se realiza durante la primera ronda y la mitad de la segunda. En la primera ronda, en lugar de contactar con $(N-1)$ proveedores,

Sub-Protocolo de Intercambio

Ronda			
1	$C \rightarrow P_i$	$CID, M_i, 1, COM_{(1,i)}$	$i \in [1..NP]$
1	$C \leftarrow P_i$	$CID, 1, ACC_{(1,i)}$	ACEPTACIÓN
		$CID, M_i, M_i^{'}, 1, ACC_{(1,i)}^{'}$	CONTRAOFERTA
		$CID, 1, REJ_{(1,i)}$	RECHAZO
2a	$C \rightarrow P_r$	$CID, 2, REJ_{(2,r)}$	$r \in \overline{RP}$
	$C \leftarrow P_r$	$CID, 2, ACKR_{(2,r)}$	
2b	$C \rightarrow P_i$	$CID, 2, COM_{(2,i)}$	$i \in \overline{AP}$
	$C \leftarrow P_i$	$CID, 2, ACC_{(2,i)}$	
⋮	⋮	⋮	
n	$C \rightarrow P_i$	$CID, n, COM_{(n,i)}$	
n	$C \leftarrow P_i$	$CID, n, ACC_{(n,i)}$	
⋮	⋮	⋮	
N	$C \rightarrow P_i$	$CID, N, COM_{(N,i)}$	
N	$C \leftarrow P_i$	$CID, N, ACC_{(N,i)}$	

$COM_{(n,i)} = S_C[CID, h(M_i), n]$
$ACC_{(n,i)} = S_{P_i}[CID, h(M_i), n]$
$ACC^{'}_{(n,i)} = S_{P_i}[CID, h(M_i), h(M_i^{'}), n]$

$ACKR_{(2,r)} = S_{P_r}[CID, h(M_r), 2, ACK - REJECTED]$
$REJ_{(z,i)} = S_{X_i}[CID, h(M_i), z, REJECTED]$;
$z = 1 \rightarrow X_i = P_i$; $z = 2 \rightarrow X_i = C$

Tabla I
SUB-PROTOCOLO DE INTERCAMBIO ATÓMICO MULTI-TWO-PARTY

Sub-Protocolo de Resolución

Consumidor $\mathbf{peticionResolucion_{(n,i)}}$
$CID, h(M_i), n$
$COM_{(1,1)}, ACC_{(1,1)}, ..., COM_{(1,(N-1))}, ACC_{(1,(N-1))}$
⋮ ⋮ ⋮
$COM_{(n,1)}, ACC_{(n,1)}, ..., COM_{(n,i)}, EVRES_{(n,i)}$

Proveedor $\mathbf{P_i}$ $\mathbf{peticionResolucion_{(n,i)}}$
$CID, h(M_i), n$
$COM_{(1,i)}, ACC_{(1,i)}, ..., COM_{(n,i)}, ACC_{(n,i)}, EVRES_{(n,i)}$

TTP $\mathbf{RespuestaResolucionCancelada_{(n,i)}}$
$Canceled_{TK} = S_{TTP}[CID, h(M_i), n, canceled]$

TTP $\mathbf{RespuestaResolucionFirmada_{(n,i)}}$
Consumer $Signed_{TK} = S_{TTP}[CID, h(M_i), n, COM_{(n,i)}]$
Provider $Signed_{TK} = S_{TTP}[CID, h(M_i), n, ACC_{(n,i)}]$

N = número de participantes; n = ronda
$COM_{(n,i)} = S_C[CID, h(M_i), n]$
$ACC_{(n,i)} = S_{P_i}[CID, h(M_i), n]$
$EVRES_{(n,i)} = S_{(C\ or\ P_i)}[CID, h(M_i), n, ...]$, firma sobre el mensaje enviado.

Tabla II
SUB-PROTOCOLO DE RESOLUCIÓN MULTI-TWO-PARTY ATÓMICO

el consumidor contactará con un número $NP \geq (N-1)$, y el mensaje M_i enviado será una propuesta de contrato. Los proveedores podrán rechazar la oferta (REJ), aceptar la oferta (ACC), o enviar una contraoferta ($ACC^{'}$). Una vez el consumidor ha recibido suficientes respuestas (al menos una positiva por servicio que desee), escogerá entre ellas las $(N-1)$ que más le interesen para continuar la ejecución del protocolo. La siguiente ronda (la número 2) se ejecutará en dos fases. Primero ($2a$), el consumidor informará a los proveedores P_r ($r \in \overline{RP}$) que no hayan sido escogidos, enviándoles un mensaje REJ, y éstos contestarán indicando que han recibido el mensaje, $ACKR$. A continuación ($2b$), el consumidor esperará a recibir todas las respuestas de los P_r descartados. Por cada P_r que no conteste, el consumidor enviará una petición a la TTP para informar de que estos proveedores han sido descartados (ver tabla III). En la segunda parte de la segunda ronda (ver ronda 2b en tabla I), el consumidor continuará la ejecución del protocolo con los $(N-1)$ proveedores escogidos (P_i $i \in \overline{AP}$), intercambiando mensajes de compromiso y aceptación, hasta conseguir el compromiso correspondiente a la ronda N, evidencia de firma.

V-B. Sub-Protocolo de Resolución

Al igual que en el protocolo AM2P original [1], consumidor y proveedores pueden contactar con la TTP en cualquier momento. Durante la primera ronda ($n = 1$), cualquier participante puede contactar con la TTP y solicitar que se cancele la firma, mientras que si $n > 1$, la petición tendrá como objetivo finalizar el protocolo (firmar el contrato). El subprotocolo de resolución (tabla II) es igual al del protocolo original [1], con una función añadida, el informe por parte del consumidor de que un proveedor P_r ha sido descartado. En la tabla III vemos el mensaje de petición y respuesta del informe de reachazo. Esta petición es necesaria para evitar que un P_r ($r \in \overline{RP}$) que ha sido rechazado por el cliente pueda obtener una evidencia de firma de la TTP y forzar su cumplimiento.

Al igual que en el protocolo orignial [1], la TTP utiliza un conjunto de reglas para solucionar correctamente las peticiones de *resolución* recibidas. Estas reglas deben aplicarse en un cierto orden, como se muestra a continuación:

- **R0** La TTP sólo aceptará una petición de resolución por participante y CID. En el caso del consumidor, las peticiones de rechazo no se contabilizarán.
- **R1** Si la TTP recibe una petición de un participante X_i durante la ronda $n = 1$, y la ejecución no ha sido previamente finalizada (*signed=true*) por otro participante ni X_i ha sido informado como rechazado por el consumidor C, la TTP cancelará la firma y le enviará a X_i una prueba de que la firma ha sido cancelada.
- **R2** Si la TTP recibe una petición de X_i durante la ronda $n > 1$, y la ejecución no ha sido previamente cancelada por otro participante ni X_i ha sido informado como rechazado por el consumidor C, la TTP la finalizará (*signed=true*) y le enviará a X_i una prueba de que el contrato está firmado.
- **R3** Si la TTP recibe una petición de X_i durante la ronda $n = 1$, y la ejecución ha sido previamente finalizada (*signed=true*) por otro participante y X_i no ha sido informado como rechazado por el consumidor C, la

Sub-Protocolo de Resolución: Informe Rechazo	
$C \rightarrow TTP$	$CID, h(M_i), COM_{(1,1)}, REJ_{(2,r)}$
$C \leftarrow TTP$	$ACK_{TK} = S_{TTP}[CID, h(M_i), 2, REJECTED]$

Tabla III
SUB-PROTOCOLO DE RESOLUCIÓN MULTI-TWO-PARTY ATÓMICO, INFORME DE RECHAZO

TTP enviará a X_i una prueba de que el contrato está firmado.

R4 Si la TTP recibe una petición de X_i durante una ronda $n > 1$, y la ejecución ha sido previamente cancelada por otro participante, la TTP revisará las peticiones previamente recibidas para comprobar si alguien ha hecho trampas. Si la TTP decide que todas las peticiones anteriores eran incorrectas, cambiará el estado de la ejecución a *signed=true* y enviará la correspondiente prueba de firma a X_i. De lo contrario, el estado continuará siendo *canceled=true* y la TTP enviará a X_i la correspondiente prueba de cancelación.

VI. REVISIÓN DE SEGURIDAD

En esta sección comprobaremos si nuestra propuesta cumple con los requisitos de seguridad para protocolos de Intercambio Equitativo Multi-Two-Party Atómicos, aplicados a la firma digital de contratos, definidos en la sección III: efectividad, equitatividad, temporalidad, no-repudio, verificabilidad de la TTP y confidencialidad.

Efectividad. La ejecución del sub-protocolo de *intercambio* (tabla I) nos asegura que, si todos los participantes actúan correctamente, el consumidor recibirá la firma de los $N-1$ proveedores escogidos, y cada proveedor $P_i, i \in \overline{AP}$ recibirá su correspondiente firma del consumidor C después de N rondas y sin intervención de la TTP. Además, todos los proveedores descartados $P_r, r \in \overline{RP}$ recibirán evidencia de que no participa en la firma del contrato M_r. Por lo tanto, el protocolo cumple con el requisito de efectividad.

Equitatividad Débil Multi-Two-Party Atómica. Si consideramos al consumidor honesto, con independencia del comportamiento del proveedor, el consumidor mantendrá la equitatividad. Hay tres posibilidades en las que un proveedor P_i (con $1 \leq i \leq (N-1)$) puede obtener una prueba de firma del consumidor:

- Después de recibir el N-ésimo compromiso $COM_{(N,i)}$, $(1 < i < (N-1))$, lo que significa que el consumidor tiene $N-1$ aceptaciones del proveedor, con lo que puede contactar con la TTP y obtener una evidencia de firma.
- Después de contactar con la TTP, lo que implica que la variable *signed* es igual a *true*, por lo tanto, el consumidor puede obtener una evidencia de firma del proveedor o de la TTP (aplicando **R3**), si el proveedor decide no continuar la secuencia de N rondas.
- Un proveedor descartado podría hacer trampas y conseguir una firma de la TTP, siguiento el ejemplo de abort-chaining (explicado en [1]). Pero si ha sido descartado por el consumidor, este tendrá o bien el mensaje $ACKR$ del propio consumidor, o el ACK_{TK} de la TTP, con lo que podrá demostrar que el proveedor hizo trampas.

En ambas situaciones, el consumidor mantiene la equitatividad.

Si consideramos un proveedor honesto P_i $(1 \leq i \leq (N-1))$, con independencia del comportamiento del consumidor, el proveedor mantendrá la equitatividad. El consumidor puede obtener una prueba de firma del proveedor de tres maneras distintas:

- Después de recibir la N-ésima aceptación del proveedor $ACC_{(N,i)}$, lo que implica que el proveedor ya tiene la prueba de firma del consumidor $COM_{(N,i)}$.
- Contactando con la TTP en la ronda $n > 1$ (aplicando **R2**), lo que quiere decir que la TTP tiene la variable *signed = true*. Por lo tanto, el proveedor podrá obtener la prueba de firma del mismo consumidor, o de la TTP (aplicando **R3**) si el consumidor decide interrumpir la secuencia de N rondas.
- Un consumidor tramposo puede descartar a un proveedor (REJ) y luego contactar con la TTP reclamando la firma del contrato con ese proveedor (aplicando **R2**). En este caso, la firma obtenida por el consumidor no tendría validez, puesto que el proveedor puede demostrar que fue rechazado, utilizando el mensaje REJ recibido.

En todas las situaciones el proveedor mantiene la equitatividad. Por lo tanto, podemos afirmar que el protocolo cumple con el requisito de Equitatividad Débil Multi-Two-Party Atómica.

Temporalidad. En cualquier momento durante la ejecución del protocolo, cualquier participante puede ejecutar el sub-protocolo de *resolución* y finalizar su ejecución, obteniendo una prueba o bien de firma, o bien de cancelación. Si todos los participantes se comportan de manera correcta el protocolo requiere de N rondas y $4NP + 2(N-1)(N-2)$ mensajes, siendo N un número finito y conocido. Por lo tanto, podemos afirmar que el protocolo tiene una duración finita, ya sea porque interviene la TTP, o por la ejecución normal de este. Es más, una vez el protocolo ha terminado, su estado final no puede cambiar. Si el protocolo finaliza con la intervención de la TTP, esta se encargará de mantener la coherencia entre las distintas peticiones posibles recibidas (siguiendo las reglas de la TTP). Si el protocolo ha finalizado después de la N-ésima ronda, las evidencias obtenidas por proveedor y consumidor servirán como prueba de su estado final. Por tanto, podemos afirmar que el protocolo cumple con el requisito de temporalidad.

No-repudio. Durante la negociación+firma de un contrato Multi-Two-Party Atómico, se generan, en cada ronda, evidencias de la participación del consumidor y de los proveedores. Por un lado tenemos los mensajes $COM_{(n,i)}$ y

los $ACC_{(n,i)}$, que relacionan a consumidores y proveedores con la firma de un contrato, y por otra parte los mensajes REJ y $ACKR$ que prueban lo contrario. En particular, el N-ésimo compromiso y la N-ésima aceptación, son considerados como la firma del contrato. Si un consumidor intenta desvincularse de la firma de un contrato M_i con el proveedor P_i, este puede probar la implicación del consumidor utilizando la firma realizada por el propio consumidor, o una evidencia obtenida de la TTP. De la misma manera, si el proveedor intenta desvincularse, el consumidor puede probar su implicación utilizando la firma generada por el proveedor, o las evidencias recibidas de la TTP.

Verificabilidad. La TTP puede comportarse de forma deshonesta y generar evidencias erróneas, dando como resultado, que algún participante honesto pueda perder su equitatividad. Suponiendo que el consumidor es honesto y la TTP deshonesta, pueden darse las siguientes situaciones:

- El consumidor envía una petición de *resolución* en la ronda $n = 1$, y la TTP contesta con una evidencia de firma. De acuerdo a las reglas de la TTP, durante la ronda $n = 1$ los participantes sólo pueden obtener prueba de cancelación. Por lo que el consumidor sabrá que la TTP ha enviado una respuesta equivocada (el consumidor no ha enviado ningún mensaje de ronda 2). Para probarlo, el consumidor puede pedirle a la TTP que presente las pruebas de la petición de resolución recibida previamente, esto es, pruebas de la ronda 2.
- El consumidor envía una petición durante la ronda $n \geq 2$ porque uno o más proveedores no han enviado su mensaje de aceptación, y la TTP responde con una evidencia de cancelación (sin que haya habido una cancelación previa), o de firma (habiendo recibido una cancelación previa). Como estamos en la ronda $n \geq 2$, las reglas de la TTP establecen que la respuesta debe ser una evidencia de firma a no ser que algún otro participante la haya cancelado, por lo tanto, cualquier respuesta es válida. Pero las evidencias contradictorias que la TTP haya enviado al consumidor y a uno o más proveedores probará la irregularidad en el comportamiento de la TTP.
- La TTP envía una evidencia de firma a un proveedor que ha sido previamente descartado (el consumidor ha informado a la TTP) por el consumidor. En este caso el consumidor podrá demostrar que la TTP ha emitido evidencias erróneas, presentando el ACK_{TK} recibido como respuesta al mensaje de informe de rechazo.

Suponiendo un proveedor honesto y la TTP deshonesta, puede darse la siguiente situación:

- El proveedor envía una petición de *resolución* durante la ejecución de la ronda n porque no ha recibido el compromiso de la ronda $(n+1)$ y la TTP responde con una cancelación (sin que haya habido una cancelación previa), o una firma (habiendo recibido una cancelación previa). Ambos resultados son coherentes con las reglas de la TTP, pero en ambos casos el proveedor y el consumidor tendrán evidencias contradictorias enviadas y firmadas por la TTP, lo que probará su mal comportamiento.
- La TTP envía una evidencia de firma a un consumidor, al que el proveedor ha rechazado previamente. Si el consumidor intenta forzar la ejecución del contrato, el proveedor podrá reclamar a la TTP que presente evidencias de aceptación, el mensaje $ACC_{(1,i)}$. Como el proveedor no ha enviado nunca este mensaje (ha enviado un $REJ_{(1,i)}$), podrá demostrar que la TTP y el consumidor se han comportado deshonestamente.

Confidencialidad. La ejecución del sub-protocolo de *resolución* no requiere el envío del texto en claro del contrato (M_i), es decir, sin cifrar. La TTP sólo recibe el resultado de aplicar una función de "hash" sobre M_i. Además, las comunicaciones entre consumidor y proveedor son punto-a-punto: del consumidor al proveedor P_i. Estrictamente hablando, para conseguir la confidencialidad deberíamos cifrar el contrato M_i, para prevenir que una tercera parte pueda monitorizar el canal de comunicaciones, y obtener su contenido. Pero esto puede evitarse utilizando algún tipo de protocolo, como Secure Socket Layer (SSL). Por lo tanto, podemos afirmar que el protocolo cumple con el requisito de confidencialidad.

VII. Conclusiones

En este artículo hemos presentado una modificación sobre un protocolo optimista para la firma electrónica de contratos en escenarios Multi-Two-Party Atómicos, que permite fusionar las fases de negociación y firma. La modificación presentada cumple con los mismos requisitos de seguridad que el protocolo original: efectividad, equitatividad, temporalidad, no-repudio y verificabilidad de la TTP. Finalmente, hemos presentado un escenario práctico en el cual podría aplicarse nuestra solución de *smart-shopping*.

Referencias

[1] G. Draper-Gil, J.-L. Ferrer-Gomila, M. F. Hinarejos, J. A. Onieva, and J. López, "Un protocolo para la firma de contratos en escenarios multi-two-party con atomicidad," in *XIIIa Reunión Española Sobre Criptología y Seguridad de la Información (RECSI XIII)*, (Arrasate, Mondragon, ES), pp. 357–362, Servicio Editorial de Mondragon Unibertsitatea, 2012.

[2] U. S. T. Committee, "Universal description, discovery and integration v3.0.2 (uddi)." http://uddi.org/pubs/uddi-v3.0.2-20041019.htm, 10 2004.

[3] N. Asokan, V. Shoup, and M. Waidner, "Optimistic fair exchange of digital signatures," in *Advances in Cryptology - EUROCRYPT'98*, vol. 1403 of *Lecture Notes in Computer Science*, pp. 591 – 606, Springer Berlin / Heidelberg, 1998.

[4] J. Zhou, R. Deng, and F. Bao, "Some remarks on a fair exchange protocol," in *Public Key Cryptography*, vol. 1751 of *Lecture Notes in Computer Science*, pp. 46 – 57, Springer Berlin / Heidelberg, 2000.

[5] Y. Liu, "An optimistic fair protocol for aggregate exchange," in *Proceedings of the 2009 Second International Conference on Future Information Technology and Management Engineering*, FITME'09, (Los Alamitos, CA, USA), pp. 564–567, IEEE Computer Society, 2009.

[6] J. A. Onieva, J. Zhou, M. Carbonell, and J. Lopez, "A multi-party non-repudiation protocol for exchange of different messages," in *18th IFIP International Information Security Conference. Security and Privacy in the Age of Uncertainty (IFIP SEC'03)*, IFIP Conference Proceedings, pp. 37–48, IFIP, 2003.