

SUMARIO

Diseño de Protocolos de No Repudio

*Jorge Dávila Muro**
CriptoLab-Facultad de Informática
UNIVERSIDAD POLITÉCNICA DE MADRID
*Javier López Muñoz**
*Felipe Roselló Ramos**
Dpto. Lenguajes y Cias. Computación
UNIVERSIDAD DE MÁLAGA
**Grupo de Trabajo de la AECSE*

Esquemas criptográficos visuales

Luis Hernández Encinas
Dpto. Didáctica de las Matemáticas
UNIVERSIDAD DE SALAMANCA
Fausto Montoya Vitini
Jaime Muñoz Masqué
Dpto. Tratamiento de la Información y Codificación
INSTITUTO DE FÍSICA APLICADA, C.S.I.C.

Los servicios de no-repudio son procedimientos que protegen a cualesquiera de las partes involucradas en una comunicación de que alguna de las demás tenga éxito al negar ilegítimamente que un determinado evento o acción haya tenido lugar. Se están convirtiendo rápidamente en servicios de gran importancia debido al crecimiento del volumen de negocios electrónicos a través de Internet, pues son capaces de producir, validar, mantener y poner a disposición de las partes, pruebas o evidencias irrefutables respecto a la transferencia de un mensaje y su contenido. Este trabajo se introduce en la compleja problemática del diseño de protocolos de no-repudio, problemática que se debe, fundamentalmente, a la diversidad de situaciones que se pueden presentar dependiendo de las características de la infraestructura de comunicación, los requerimientos de las entidades que intervienen en ella y el propio comportamiento de éstas. El estudio llevado a cabo clasifica protocolos ya existentes e identifica en qué situaciones se deben emplear cada uno de ellos.

Diseño de Protocolos de No-Repudio

Introducción

El repudio es una de las amenazas de seguridad que pueden aparecer en el mundo de las transacciones comerciales basadas en papel. Documentos tales como contratos, órdenes de compra, facturas o cheques tienen un papel trascendental en la forma de realizar los negocios entre las empresas. Sin embargo, la manipulación de esos tipos de documentos puede originar graves problemas derivados de falsificaciones, modificaciones accidentales o intencionadas, pérdidas o retrasos postales, disputas sobre el momento exacto de envío o recepción, etc.

Tras estos problemas suelen ocultarse comportamientos fraudulentos donde alguna de las partes implicadas reniega de la autoría de algún documento, del envío o recepción del mismo o, quizá, del instante exacto en que tales hechos tuvieron lugar. Para impedir o, al menos, dificultar estos comportamientos ilegítimos se utilizan mecanismos tan habituales como firmas manuscritas, recibos timbrados, mata-sellos, correo postal certificado, e incluso la participación de fedatarios públicos.

En las transacciones comerciales realizadas a través de procedimientos electrónicos los inconvenientes que pueden aparecer, de seguridad en general, y de repudio en particular, son equivalentes a los anteriormente mencionados. En algunos aspectos son, incluso, más difíciles de resolver que sus análogos en las transacciones basadas en documentos de papel. Estas dificultades añadidas son debidas, fundamentalmente, a que las entidades están distribuidas en distintos lugares y bajo normativas distintas, las transacciones no se realizan en persona, y en ningún caso hay evidencia física de la transacción.

Para satisfacer los requerimientos de seguridad de las aplicaciones electrónicas se han definido tradicionalmente cinco categorías de servicios de seguridad [1]. De ellos, los servicios de autenticación, control de acceso, confidencialidad, e integridad de datos han sido objeto de un intenso y

amplio estudio. El quinto servicio, que está directamente asociado a los problemas mencionados en los párrafos anteriores, es el servicio de no-repudio, para el que la investigación no ha sido tan exhaustiva como en los demás. Precisamente, los objetivos de seguridad de las nuevas formas de negocios electrónicos entre empresas, el contacto con los bancos a través de Internet, y la interrelación de los ciudadanos con las Administraciones Públicas hace imprescindible el estudio de este servicio.

Poder vincular la responsabilidad del autor a lo que hace es un aspecto importante de la Seguridad de la Información, especialmente si hablamos de un entorno comercial o contractual. Por ello, al utilizar un entorno de comunicación distribuido es necesario evitar que las entidades puedan negar con éxito haber enviado o recibido ciertos mensajes de contenido comprometedor para ellas; es decir, es necesario poder responsabilizar a cada cual de sus compromisos adquiridos y de sus acciones. Por lo tanto, puede entenderse el repudio como la negación por parte de alguna de las entidades involucradas en una comunicación de haber intervenido en toda o en parte de ella. A partir de esto puede establecerse que el servicio de no-repudio es el procedimiento que protege a cualesquiera de las partes involucradas en una comunicación de que alguna de las demás tenga éxito al negar ilegítimamente que un determinado evento o acción haya tenido lugar. Para ello, el servicio ha de producir, validar, mantener, y poner a disposición de las partes, pruebas o evidencias irrefutables respecto a la transferencia de información desde el emisor al receptor y del contenido de ésta.

El servicio de no-repudio está íntimamente relacionado con el servicio de autenticación, pero el primero tiene que cumplir más requisitos que el segundo en cuanto a las pruebas que ha de producir. La diferencia esencial entre ambos es que la autenticación sólo necesita convencer a la otra parte involucrada en la comunicación de la validez de un evento y de su autoría, mientras que el no-repudio, ade-

más, ha de probar esas mismas cualidades frente a una tercera parte que no participa en la comunicación cuando ésta se produce. Es decir, y esto es esencial, el propósito principal del servicio de no-repudio no es el de proteger a los usuarios ante ataques externos, sino de las amenazas de otros usuarios legítimos.

En general, este servicio está dirigido a resolver desacuerdos del tipo de si un determinado evento ocurrió o no, cuándo tuvo lugar, qué entidades intervinieron en dicho evento y cuál era la información asociada a él. El punto clave de los servicios de no-repudio es que las partes han de obtener suficientes pruebas para resolver sus diferencias, entre ellas mismas, o empleando algún tipo de arbitraje. Para la construcción de este tipo de servicios y de sus pruebas se hace uso de mecanismos criptográficos tales como la firma digital, el cifrado de mensajes, los códigos de autenticación de mensajes (MACs) y la notarización de documentos, además de otros servicios clásicos de seguridad.

Tipos de No-repudio

Hasta el momento se ha tratado el servicio de no-repudio en forma singular, pero en realidad se debería pluralizar y hablar genéricamente de servicios de no-repudio ya que, como se verá a continuación, existen diversos tipos, cada uno con un cometido particular. A este respecto debemos referirnos a los estándares internacionales relacionados con el no-repudio: ISO/IEC 10181-4 [2] e ISO/IEC 13888 [3, 4, 5]. El primero de ellos extiende el concepto de servicios de no-repudio descrito en [1] y proporciona un marco de trabajo para el desarrollo y provisión de estos servicios. El segundo se compone de tres partes, la primera de las cuales proporciona un modelo general de no-repudio, mientras que las otras dos proporcionan un conjunto de mecanismos de no-repudio basado en técnicas criptográficas simétricas y asimétricas.

Si simplificamos una comunicación a su mínima expresión, las entidades que intervienen son el emisor y el receptor del mensaje. Los dos servicios de no-repudio que se pueden definir en este escenario son:

- No-repudio de origen. Este servicio proporciona al receptor de un objeto digital una prueba infalsificable del origen de dicho objeto, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario.
- No-repudio de recepción. Proporciona al emisor la prueba de que el destinatario legítimo de un mensaje u objeto digital genérico, realmente lo recibió, evitando que el receptor lo niegue posteriormente y consiga sus pretensiones. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

Existen escenarios, como los sistemas de administración de mensajes (sistemas de correo) y muchas de las aplicaciones de comercio-e, donde se ha de garantizar la entrega eficiente, confiable y segura tanto de pagos como de productos digitales, y donde se han de proporcionar evidencias apropiadas de tales hechos para solucionar posibles disputas y discrepancias posteriores. En muchas de las comunicaciones de este tipo interviene, además, una Tercera Parte Confiable (TTP), y su actuación puede dar lugar a dos servicios adicionales de no-repudio:

- No-repudio de presentación. Este servicio proporciona al emisor la prueba de haber revelado el mensaje a la TTP, imparcial y confiable, la cual genera la prueba.
- No-repudio de entrega. En este caso el sistema proporciona al emisor la prueba de que la propia TTP ha entregado el mensaje al receptor especificado originalmente y sólo a él. Esta prueba también la aporta la TTP basándose en su aceptada imparcialidad y buen hacer.

Pruebas o evidencias

Con anterioridad se ha hecho hincapié en el concepto de prueba (e indistintamente en el de evidencia), pero no se ha definido apropiadamente. Se puede deducir de todo lo dicho hasta aquí que las pruebas son los elementos fundamentales de los servicios de no-repudio. Pero, más en detalle, puede observarse que lo que exactamente han de proporcionar es información suficiente sobre la ocurrencia de un evento, el momento en el que ocurrió y qué partes intervinieron.

Por ello, las evidencias de no-repudio relativas a la transferencia de un mensaje incluyen los siguientes elementos, algunos de los cuales son opcionales y dependen de la aplicación: el tipo de servicio de no repudio que se proporciona, la identidad incontestable del emisor y del receptor, el identificador del que genera la evidencia (si es diferente del emisor o del receptor), los identificadores de otras terceras partes involucradas, el mensaje a transmitir o algo indisoluble asociado con él, una estampilla digital de tiempo indicando cuándo se generó un mensaje, otra indicando cuando se realizó la transferencia del mismo, y la fecha de expiración o caducidad de la evidencia.

Desde el punto de vista de la evidencia, un servicio de no-repudio está compuesto por cuatro fases distintas. En primer lugar, la fase de generación de la evidencia, que puede ser realizada por cualquiera de las entidades pues sólo se requiere que éstas firmen digitalmente porciones determinadas de información; en segundo lugar, la fase de transferencia; en tercer lugar, la fase de verificación y almacenamiento de la evidencia, que consiste en comprobar la firma digital y guardar la información para un uso posterior; y, por último, la fase de resolución de disputas, en caso de que éstas tengan lugar.

El papel de las TTPs en los servicios de No-repudio

Ya es sabido que, por definición, una TTP es una autoridad, o agente especial en el que confían las demás entidades respecto a su seguridad y correctas pautas de actuación. Las TTPs juegan un papel importante en muchas propuestas de no-repudio. Dependiendo de la política de no-repudio y de los mecanismos utilizados pueden distinguirse varias clases de TTPs. Cada una de ellas participa de distinta forma para ayudar a las entidades a generar, verificar y transferir evidencias de no-repudio y, en el caso de ser necesario, resolver disputas. La taxonomía de este tipo de agentes, siempre desde el punto de vista de los servicios de no-repudio, es la siguiente:

- Autoridad de Certificación. Son TTPs generadoras de certificados de clave pública que garantizan el vínculo entre las claves de verificación de firmas utilizadas con propósitos de no-repudio y la identidad no digital (física o jurídica) de cada uno de los participantes. También proporcionan puntualmente Listas de Revocación de Certificados para mantener informados a todos los agentes competentes de la continuada validez de los certificados emitidos, y para determinar la validez de las claves antiguas (ya caducadas). Dentro de un servicio de no-repudio una Autoridad de Certificación no suele trabajar en modo interactivo, sino diferido.
- Notario. Representa a las diferentes entidades, las cuales confían en dicho agente para proporcionar las evidencias adecuadas o para verificar correctamente otras que se producen durante la transacción. Las propiedades de cualquier mensaje intercambiado entre las entidades, tales como las de origen y de integridad, se pueden garantizar mediante la intervención del notario, que funciona en modo interactivo y que, además, puede proporcionar u obtener sellos digitales de tiempo referidos al momento de generación de la evidencia.

- Agente de Entrega . Su misión es la entrega certificada de mensajes de una entidad a otra y, con ello, proporciona las correspondientes evidencias. Su funcionamiento, lógicamente, es interactivo.

- Juez: Su único cometido es el de resolver disputas cuando éstas se plantean sobre la ocurrencia o no de un determinado evento. Para ello, recurre a la evaluación personal de las evidencias que presentan los litigantes y siempre sujeto a una política determinada de no-repudio. Un juez no se implica en el servicio de no-repudio a menos que haya una disputa que resolver y se precise de un arbitraje imparcial, por lo que su funcionamiento es en modo diferido.

Diseño de Protocolos

Las características de la infraestructura de comunicación, los requerimientos de las entidades que intervienen en ella y el propio comportamiento (honrado o no) de éstas da lugar a un amplio y complejo conjunto de situaciones, algunas de las cuales se presentan diametralmente opuestas. Por lo tanto, el diseño de protocolos de no-repudio resulta complejo pues la confección de los mismos no viene determinada por aspectos generales, sino por aspectos específicos que condicionan, por ejemplo, el número de mensajes intercambiados, la longitud de esos mensajes o la necesidad de intervención de terceras partes.

En este apartado se describen diversos protocolos y cada uno de ellos pretende dar una solución a una situación diferente de las demás. Se muestra, a partir de un caso básico, cómo va aumentando la complejidad en el diseño de estos protocolos a medida que se incrementan los requerimientos de las entidades y varían las condiciones en las que éstas interactúan.

Se ha empleado una breve notación básica para todos los protocolos. Aquellas expresiones propias de cada protocolo son explicadas durante la descripción del mismo. La notación básica es la siguiente:

- H_M : función resumen aplicada al mensaje M;
- $S_X(M)$: firma digital de la entidad X sobre el mensaje M;
- $X \bar{O} Y : M$: la entidad X envía el mensaje M a la entidad Y;
- $X \bar{O} TTP : M$: la entidad X obtiene M de la TTP (mediante ftp o a través de Web).

Se parte de la base de que las dos entidades de la comunicación han de obtener un acuse de recibo cada vez que envían un mensaje. Ese recibo es el que emplearán como prueba. Asimismo, se considerarán dos posibles razones por las que el recibo podría no llegar; bien porque el canal de comunicaciones introduce fallos (no es fiable), o bien porque alguna de las partes no actúa honradamente (por no seguir las reglas del protocolo o por abandonar la ejecución del protocolo de forma intencionada). Además, en todos los protocolos se considera que la entidad receptora no tiene capacidad de espiar en la red y, por lo tanto, de obtener ilícitamente algunos de los mensajes que no van dirigidos a ella.

• Protocolo 1

Aquí se supone una situación ideal en la que el canal de comunicación es perfectamente fiable y todas las partes se comportan de forma honrada. En este caso el protocolo es muy simple:

1. $A \bar{O} B$: $B, M, S_A(B, H_M)$
2. $B \bar{O} A$: $A, S_B(A, H_M)$

Las firmas de A y B sirven como pruebas de origen y

recepción respectivamente.

• Protocolo 2

Siguiendo bajo la suposición de que el canal de comunicación es fiable, ahora se considerará que las entidades no actúan de forma honrada. En este caso el protocolo anterior deja a B en una situación ventajosa porque puede leer el mensaje antes de enviarle a A el recibo o prueba de recepción. Este problema se conoce como recepción selectiva (una de las entidades puede decidir si le conviene confirmar o no el mensaje que le ha llegado), y se puede solucionar involucrando en la transferencia a una TTP de la siguiente forma:

1. $A \bar{O} TTP$: $TTP, B, M, S_A(TTP, B, H_M)$
2. $TTP \bar{O} B$: $A, B, M, S_{TTP}(A, B, H_M)$
3. $TTP \bar{O} A$: $A, B, S_{TTP}(A, B, H_M)$

La TTP actúa como Agente de Entrega. Sus firmas digitales sirven como prueba de presentación y como prueba de entrega (en lugar de las anteriores pruebas de origen y de recepción).

• Protocolo 3

En este caso se supondrá que las entidades se comportan de forma honrada, pero es el canal de comunicación el que no aporta fiabilidad. El protocolo para esta situación es el siguiente:

1. $A \bar{O} B$: $B, M, S_A(B, H_M)$
2. $B \bar{O} A$: $A, S_B(A, H_M)$
3. $A \bar{O} B$: $B, S_A(ACK, B, H_M)$

El paso 2 se repite tantas veces como sea necesario hasta que el canal permita a B obtener la etiqueta de reconocimiento ACK (Acknowledge) generada por A en el paso 3.

• Protocolo 4

Si el canal de comunicación no es fiable y además las entidades tampoco son honradas los dos protocolos anteriores no son útiles porque dejan en una posición de ventaja a B frente a A. Por un lado, en el protocolo 2, B puede negar haber recibido el mensaje de la TTP. Por el otro, en el protocolo 3, B puede no enviar la prueba de recepción. Para prevenir estos problemas el protocolo puede comenzar con una promesa de intercambio, de forma que en una primera instancia se envía el mensaje cifrado, C, y en un paso posterior

se envía la clave K, con la que se ha cifrado M. El protocolo es:

1. $A \bar{O} B$: $B, C, S_A(B, H_C)$
2. $B \bar{O} A$: $A, S_B(A, H_C)$
3. $A \bar{O} B$: $B, K, S_A(B, K)$
4. $B \bar{O} A$: $A, S_B(A, K)$

Pero este protocolo, tal y como está, no garantiza que B ejecute realmente el paso 4, por lo que se quedaría en ventaja respecto a A, y ésta se podría quedar sin su prueba de recepción. Por lo tanto, el protocolo no es adecuado para la situación preestablecida, a no ser que, como propone la ISO (autora del protocolo), nos basemos en la propiedad de continuidad. Esta propiedad indica que si B obtiene la clave K en el paso 3 entonces se verá obligado a ejecutar el paso 4 ya que, en el caso de no hacerlo, el juez resolverá contra B en cualquier posible disputa posterior que A inicie. Con el uso de esta premisa se puede justificar que el protocolo efectivamente puede ser empleado para resolver la situación propuesta. Con dicha premisa el protocolo descrito en [6] también la resuelve.

• Protocolo 5

En ciertas aplicaciones puede no ser conveniente confiar en propiedades que, desde un punto de vista teórico, son completamente externas al protocolo, como es el caso de la propiedad de continuidad. Esta, además, también puede re-

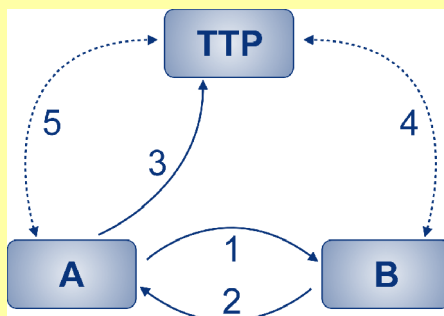


Figura 1. Ejemplo de TTP actuando como Notario

sultar bastante peligrosa desde un punto de vista práctico. Por lo tanto, en esas circunstancias, el problema de que una entidad quede en desventaja frente a la otra ha de resolverse dentro del mismo protocolo. Es necesario un protocolo imparcial, es decir, un protocolo de no-repudio que, tras su correcta finalización, haya proporcionado pruebas irrefutables tanto al autor del mensaje como al receptor, sin que ninguno de ellos haya quedado en una posición ventajosa durante la ejecución del mismo.

A continuación se expone un ejemplo de protocolo imparcial [7]. Se usa una TTP, aunque su intervención es mínima. Este protocolo también divide la definición del mensaje en dos partes: por un lado el texto cifrado C, que se utiliza como compromiso, y por otro lado la clave K con la que se ha cifrado M. El compromiso (texto cifrado) es intercambiado directamente entre A y B, pero la clave pasa a través de la TTP. Se usa la etiqueta L para distinguir los pasos que pertenecen a una misma ejecución del protocolo. Además se utilizan los términos N_O (prueba de origen), N_R (prueba de recepción), $proc_K$ (prueba de que la clave procede de A) y pub_K (prueba de que el TTP ha publicado K), cuyas expresiones respectivas son:

$$N_O = S_A(B, L, H_C); \quad N_R = S_B(A, L, H_C); \quad proc_K = S_A(B, L, K); \quad pub_K = S_{TTP}(A, B, L, K)$$

1. A \bar{O} B: B, L, C, N_O
2. B \bar{O} A: A, L, N_R
3. A \bar{O} TTP: B, L, K, $proc_K$
4. B \bar{O} TTP: A, B, L, K, pub_K
5. A \bar{O} TTP: A, B, L, K, pub_K

IV

Es necesario aclarar que una vez que la TTP recibe $proc_K$ en el paso 3, genera pub_K y almacena la tupla (A, B, L, K, pub_K) en un directorio que es accedido por A y B (el orden del acceso no es importante), ya sea a través de una conexión ftp o http. En el protocolo, la TTP no actúa como Agente de Entrega, sino más bien como Notario. Esto conlleva dos ventajas: la primera es que solamente maneja claves en lugar de largos mensajes; la segunda es que la responsabilidad de la ejecución de los últimos pasos recae directamente sobre emisor y receptor (un Agente de Entrega tendría que reenviar los mensajes hasta que los otros respondieran admitiendo haberlos recibido).

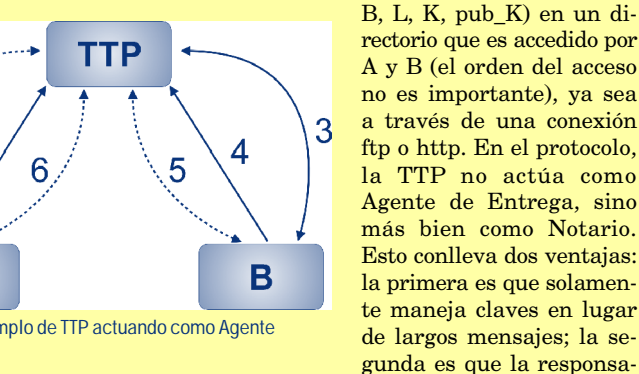


Figura 2. Ejemplo de TTP actuando como Agente de Entrega

En la práctica no es deseable que la TTP almacene indefinidamente las tuplas que contienen las claves. Se puede establecer un límite de tiempo, T_L , para acotar el periodo en que pueden ser accedidas. Ese límite es elegido por el emisor, por ser la entidad que inicia el protocolo, pero siempre tomando como referencia el reloj de la TTP. Ampliar el protocolo 5 para que contemple esta situación es algo inmediato pues basta con añadir el término T_L a las expresiones N_O , N_R , $proc_K$ y pub_K y, además, a los pasos 1 y 3. Opcionalmente, la TTP puede incluir una estampilla de tiempo para indicar el momento a partir del cual la tupla ha estado publicada y disponible en el directorio. Denotamos mediante T_D a la estampilla de disponibilidad. Esta modificación adicional al protocolo también es muy simple pues basta con añadir T_D a los pasos 4 y 5 (además de las inclusiones de T_L indicadas anteriormente).

• Protocolo 6

En algunas aplicaciones, tanto el emisor como el receptor del mensaje necesitan, junto a la prueba de origen o de destino, una prueba adicional sobre el momento exacto en el

que el mensaje se envía o se recibe. Como se ha visto en la ampliación final del protocolo 5, esa prueba puede ser proporcionada por la propia TTP. Sin embargo, en ese protocolo, A sólo puede enviar la clave K después de recibir en el segundo paso el compromiso por parte de B. Esto carga a A con toda la responsabilidad derivada de un envío tardío de la clave K a la TTP en el paso 3, ya que B puede demorar a su antojo la ejecución del paso 2. No es difícil pensar en aplicaciones de comercio electrónico donde un retraso intencionado del receptor, como el que aquí se puede producir, perjudicaría claramente al emisor. Por lo tanto, la ampliación del protocolo 5 no es útil para ese tipo de aplicaciones.

A continuación se expone un protocolo que sí cumple con el requerimiento propuesto [8]. En él se utilizan los términos T_P (momento en que la TTP ha recibido los datos de A), y T_E (momento en el que el mensaje está disponible para B). Adicionalmente, se usan los términos N_O (prueba de origen), N_R (prueba de recepción), N_P (prueba de presentación) y N_E (prueba de entrega), cuyas expresiones respectivas son:

$$N_O = S_A(TTP, B, H_M); \quad N_R = S_B(TTP, A, L, N_O); \quad N_P = S_{TTP}(A, B, T_P, L, N_O); \quad N_E = S_{TTP}(A, B, T_E, L, N_R)$$

1. A \bar{O} TTP: TTP, B, M, N_O
2. A \bar{O} TTP: A, B, T_P , L, N_P
3. TTP \bar{O} B: A, L, N_O
4. B \bar{O} TTP: L, N_R
5. B \bar{O} TTP: L, M
6. A \bar{O} TTP: T_E , L, N_R , N_E

Con objeto de prevenir que B realice una recepción selectiva, la TTP le informa (paso 3) de que existe para él un mensaje, etiquetado con L, a la espera de ser recogido. Sólo después de que B se ha comprometido a recoger ese mensaje (paso 4) la TTP publica el mensaje en el directorio. En este caso la TTP actúa como Agente de Entrega, certificando todos los envíos entre A y B.

• Protocolo 7

Existe otra cuestión, a veces crítica, que consiste en cómo mantener la validez de una prueba de no-repudio de una forma eficiente durante y después de la transacción. Como se ha visto, las pruebas de no-repudio se generan por medio de firmas digitales. En la práctica la clave de firma puede quedar comprometida y la firma puede ser falsificada. Por lo tanto, las claves comprometidas deben ser revocadas para que las firmas generadas fraudulentamente sean tomadas como inválidas. La cuestión es cómo probar que la firma realizada por una entidad dentro de un protocolo de no-repudio se ha generado antes de que el correspondiente certificado de clave pública haya sido revocado.

Una solución simple es la utilización de autoridades de fechado (TSAs) para que las entidades puedan estampillar las pruebas de origen y de recepción. Pero esta solución no es rentable para algunos tipos de transacciones en línea porque puede ocasionar un excesivo número de intercambio de mensajes dentro del protocolo. Para aplicaciones de este tipo se puede utilizar el siguiente protocolo [9]:

1. A \bar{O} B: B, L, C, N_O
2. B \bar{O} A: A, L, N_R
3. A \bar{O} TTP: B, L, $E_{TTP}(K)$, N_R , $pres_K$
4. B \bar{O} TTP: A, B, L, K, T, pub_K
5. A \bar{O} TTP: A, B, L, K, T, pub_K

$$N_O = S_A(B, L, H_C); \quad N_R = S_B(A, L, H_C, N_O); \quad pres_K = S_A(B, L, E_{TTP}(K), N_R, Cert_B); \quad pub_K = S_{TTP}(A, B, L, K, N_R, T)$$

El término $E_{TTP}(K)$ denota el cifrado de K utilizando la clave pública del TTP, mientras que C simboliza, como anteriormente, el mensaje M cifrado con la clave simétrica K. Además, $Cert_B$ representa el certificado de clave pública de B, que la propia entidad A comunica a la TTP. Se puede observar que este protocolo usa un mecanismo de encadena-

miento de pruebas, enlazando una prueba con otra, de forma que la validación de la última supone la validación de todas las anteriores. El concepto de encadenamiento no es nuevo, ya que se ha utilizado con anterioridad en la autenticación de contraseñas [10], en servicios de estampillado digital de tiempos [11] y en esquemas de micropago [12], pero su aplicación a las pruebas de no-repudio sí es original de este protocolo.

• Protocolo 8

En la mayoría de los protocolos anteriores la TTP interviene de forma muy activa. Estos protocolos son apropiados en las aplicaciones donde es necesaria la notarización de las claves, donde es esencial la imparcialidad, o donde los participantes y la infraestructura de las comunicaciones son tan poco fiables que es recomendable confiar a la TTP todo el peso del protocolo. Sin embargo, en algunos entornos se considera como objetivo de diseño del protocolo la reducción de la carga de trabajo de la TTP. Además hay otros entornos donde la confianza entre emisor y receptor es grande, de tal forma que las pruebas son intercambiadas entre ellos de forma directa, y donde los servicios de una TTP sólo se requieren como último recurso para resolver situaciones muy concretas. En estas situaciones los protocolos estudiados hasta el momento no son adecuados, sino que son necesarios otros donde la participación de la TTP sea ocasional. A continuación se muestra un ejemplo de uno de estos protocolos [13], donde el término T_L se utiliza de la misma forma que en el protocolo 5, y donde n_A y n_B representan números aleatorios que formarán parte de las pruebas de no-repudio. Además, se usan las siguientes expresiones:

$$N_O' = S_A(TTP, B, T_L, H(M, n_A), H(n_A)); N_O = N_O', n_A; N_E = S_{TTP}(A, B, T_L, M, n_A)$$

$$N_R = N_R', n_B; N_R' = S_B(TTP, A, T_L, H(M, n_A), H(n_A), H(n_B));$$

1. A \tilde{O} B: TTP, B, T_L , $H(M, n_A)$, $H(n_A)$, N_O'
2. B \tilde{O} A: $H(n_B)$, N_R'
3. A \tilde{O} B: M, n_A
4. B \tilde{O} A: n_B

Sólo en el caso de que A no reciba n_B después de haber ejecutado el paso 3, se iniciará la fase en la que interviene la TTP antes de que se llegue al límite T_L . Los pasos adicionales del protocolo que se ejecutan en ese caso son:

- 3'. A \tilde{O} TTP: TTP, B, T_L , $H(M, n_A)$, $H(n_A)$, N_O' , $H(n_B)$, N_R' , M, n_A
- 4'. TTP \tilde{O} B: M, n_A
- IF 5'. B \tilde{O} TTP: n_B
- THEN 6'. TTP \tilde{O} A: n_B
- ELSE 7'. TTP \tilde{O} A: N_E

Al igual que este protocolo, otros como [14] y [15], también están diseñados para utilizar la TTP sólo cuando es estrictamente necesario.

Conclusiones

Los servicios de no-repudio están empezando a jugar un papel trascendental en el campo de la Seguridad de la Información ya que vienen a cubrir un hueco dentro de los objetivos de seguridad que las nuevas formas de negocios electrónicos requieren. La utilización de protocolos de no-repudio garantiza que las tradicionales transacciones comerciales basadas en soporte papel como contratos, órdenes de compra, facturas o cheques, pueden ser trasladadas al entorno telemático con una mayor seguridad, incluso, que la que actualmente proporciona la manipulación de los mismos documentos en papel. Además, el hecho de trabajar con los correspondientes elementos digitales proporciona a los usuarios no sólo una mayor seguridad, sino también una mejora en la velocidad, autonomía y comodidad en la utilización de esos servicios telemáticos.

En este trabajo hemos mostrado que, a pesar de la diversidad de situaciones y requerimientos que pueden encontrarse en los entornos donde se han de utilizar las nuevas aplicaciones, la versatilidad y multiplicidad de los protocolos de no-repudio, así como la descomposición del servicio general de no-repudio en otros servicios más elementales, permiten encontrar soluciones satisfactorias para cada caso. Precisamente, en este estudio hemos realizado una clasificación de protocolos ya existentes y se han identificado, de forma clara, bajo qué condiciones se pueden utilizar con plena garantía. {fausto, jaimel}@iec.csic.es

Agradecimientos

Los autores agradecen al Dr. Jianying Zhou, de Kent Ridge Digital Labs (Singapur), sus comentarios, sugerencias y aclaraciones durante la elaboración de este trabajo, así como las recomendaciones y ayuda proporcionada para la recopilación del material más relevante sobre el tema.

✉ Jorge Dávila Muro*
 jdavila@fi.upm.es
 CriptoLab-Facultad de Informática
 UNIVERSIDAD POLITÉCNICA DE MADRID
 Javier López Muñoz*
 jlm@lcc.uma.es
 Felipe Roselló Ramos*
 crypto@lcc.uma.es
 Dpto. Lenguajes y Ciencias de la Computación
 UNIVERSIDAD DE MÁLAGA
 *Grupo de Trabajo de la AECSI

V

REFERENCIAS

- [1] ISO 7498-2. *Information processing system – Open systems interconnections – Basic reference model – Part 2: Security architecture*. International Organizations of Standardization, 1989.
- [2] ISO/IEC 10181-4. *Information technology- Open systems interconnections – Security frameworks in open systems – Part 4: Non-repudiation*. ISO/IEC, 1996.
- [3] ISO/IEC DIS 13888-1. *Information technology- Security techniques – Non repudiation - Part 1: General model*. ISO/IEC JTC1/FC27 N1503, November 1996.
- [4] ISO/IEC 5th CD 13888-2. *Information technology- Security techniques – Non repudiation - Part 2: Using symmetric techniques*. ISO/IEC JTC1/FC27 N1505, November 1996.
- [5] ISO/IEC DIS 13888-3. *Information technology- Security techniques – Non repudiation - Part 3: Using asymmetric techniques*. ISO/IEC JTC1/FC27 N1507, November 1996.
- [6] T. Coffey, P. Saidha, *Non-repudiation with mandatory proof of receipts*, Computer Communications Review, 26 (1), January 1996, pp. 6-17
- [7] J. Zhou, D. Gollman, *A Fair Non-repudiation Protocol*, Proceedings of the 1996 IEEE Symposium on Security and Privacy, 1996, pp. 55-61
- [8] J. Zhou, D. Gollman, *Observations on Non-repudiation*, Lectures Notes in Computer Science. Advances in Criptology. ASIACRYPT '96, 1996, pp. 133-144
- [9] C. H. You, K. Y. Lam, *On the efficient implementation of fair non-repudiation*, Computer Communication Review, 28(5), October 1998, pp. 50-60
- [10] L. Lamport, *Passwords authentication with insecure communication*, Communications of the ACM, 24 (11), 1981, pp. 770-772
- [11] S. Haber, S. Stornetta, *How to time-stamp a digital document*, Journal of Cryptology, 3 (2), 1991, pp. 99-111
- [12] T. Pedersen, *Electronic payments of small amounts*, Proceedings of Cambridge Workshop on Security Protocols, 1996, pp. 59-68
- [13] N. Asokan, M. Schunter, M. Waidner, *Optimistic protocols for fair exchange*, 4th ACM Conference on Computer and Communications Security, 1998, pp. 8-17
- [14] J. Zhou, D. Gollman, *An efficient Non-repudiation Protocol*, 10th IEEE Computer Security Foundations Workshop, 1997, pp. 126-132
- [15] R. Deng, F. Bao, *Evolution of fair non-repudiation with TTP*, Proceedings of 1999 Australasian Conference on Information Security and Privacy, 1999, pp. 258-269