

No cabe duda de que los servicios de notarización y los notarios electrónicos van a resultar fundamentales durante los próximos años. El hecho de que las empresas y los ciudadanos estén familiarizados con el concepto tradicional de "notario", así como con las funciones de éstos, va a contribuir significativamente a que su sustituto digital se convierta en un eslabón muy importante en la cadena de mecanismos electrónicos que conduzcan, de forma definitiva, al entorno de confianza adecuado para el desarrollo del comercio electrónico en un ámbito global. Este artículo revisa algunas propuestas anteriores relacionadas con el tema, y pretende arrojar algo de luz sobre los servicios que han de realizar estos nuevos agentes digitales.

Servicios de Notarización Electrónica

El comercio electrónico en Internet está sufriendo una expansión acelerada a la vez que desordenada, y aún va a estar sometido a cambios más vertiginosos a medida que las TIC sigan avanzando. Se va a engendrar una gran variedad de negocios y mercados innovadores, y se van a crear nuevas fuentes de ingresos, además de mejorar la eficiencia de las actividades no sólo industriales o empresariales, sino también administrativas. Buena prueba de ello es el interés despertado en los organismos oficiales europeos [1] y nacionales [2].

El problema de la seguridad se configura como piedra angular dentro del comercio electrónico. Se puede afirmar que las funciones, protocolos y servicios criptográficos conforman el conjunto de herramientas a utilizar para dotar de seguridad a los procedimientos digitales de cualquier índole. De hecho, la criptografía tiene una gran variedad de aplicaciones relacionadas con la protección de la privacidad, la propiedad intelectual, la información financiera y de negocios, la seguridad pública y la seguridad nacional.

Sin embargo, y a pesar de la existencia de estas herramientas, cuando se trata de preservar la privacidad de documentos y transacciones, se siguen utilizando redes privadas; es decir, aquellas que implican a usuarios que ya se conocen previamente y entre los que existe bastante grado de familiaridad. Obviamente, es éste un modelo que no puede ser transferido a las redes abiertas debido a la ausencia de relación previa entre sus usuarios. El resultado real, que no el que "alegremente" es difundido por muchos medios de comunicación, es que las ventajas para el desarrollo de oportunidades comerciales, tanto entre organizaciones privadas como entre las organizaciones públicas y los ciudadanos, no está siendo explotado, ni mucho menos, en su totalidad.

El principal factor inhibitor sigue siendo el recelo que infunde la red. Este recelo se debe, por un lado, a la idea generalizada de que falta una infraestructura global suficientemente segura y eficaz para soportar procedimientos también globales de identificación de usuarios y de autenticidad de los datos, y por otro lado, al riesgo y desconfianza que aparecen cuando se trata de actos con implicaciones de terceros. Claramente, se percibe que detrás de los aspectos de seguridad (que se supone se pueden acometer con garantías mediante el uso de herramientas criptográficas) está enmascarado un concepto, acaso más amplio, en torno al cual gira toda esta problemática, la confianza.

Por lo tanto, resulta muy importante que una empresa o cualquier ciudadano que utilice Internet para desarrollar sus actividades disponga de mecanismos en los que confiar y que le garanticen la seguridad, en el sentido más amplio del término, de las operaciones digitales realizadas. Así, en una situación ideal los usuarios del comercio-e deberían hacer uso de mecanismos y procedimientos electrónicos que fueran equivalentes, y ofrecieran las mismas garantías, que aquellos otros que en la sociedad actual se aplican sobre documentos en soporte papel, y en los que efectivamente confían. Es

decir, los usuarios de las redes de información digital deberían hacer uso de soportes electrónicos confiables de autenticación, autorización, privacidad, etc., con los mismos efectos que los utilizados en soporte papel.

Debido a que históricamente la figura del notario humano (así como las de otros tipos de fedatarios públicos) ha gozado de confianza por parte de los ciudadanos y de las instituciones públicas y privadas, está más que justificado trasladar al entorno digital, si no todas, sí el máximo de funciones posibles que actualmente recaen en el notario humano. De esta forma, el notario electrónico, así como una infraestructura compuesta por un número de éstos, pueden pasar a ser el primer eslabón de una cadena que ayude a crear el entorno de confianza adecuado y que garantice la seguridad y la fiabilidad del comercio a través de Internet.

CUESTIONES POR RESOLVER Y PROPUESTAS PREVIAS

El notario humano ha sido y es representación de seguridad jurídica en nuestra sociedad. Por ello, la creación y el desarrollo de nuevos procedimientos electrónicos equivalentes a los bien conocidos y tradicionales procesos notariales podrían encontrarse con algún tipo de inconveniente legal. Esto no debería ser óbice para que el desarrollo tecnológico se paralizara. De hecho, la aparición de nuevas situaciones o vinculaciones sociales ha de obligar al Derecho a adaptar las leyes a las novedades producidas, y buena prueba de ello es el Real Decreto-ley de Firma Electrónica [3].

Una vez decididos a trasladar al escenario digital las funciones del notario humano habría que precisar qué figura notarial concreta de la sociedad es necesario tomar como punto de partida, pues los sistemas de notariado presentan diferentes características dependiendo del país o grupo de países que se considere. De forma general, se pueden establecer dos grupos. Por un lado, el de aquellos cuya práctica deriva del uso notarial anglosajón y, por otro, el de aquellos cuya práctica deriva del uso notarial latino (o romano-germánico).

Con todo, para poder determinar qué figura notarial es necesario emular podría ser más conveniente plantear inicialmente un par de cuestiones. La primera de ellas se refiere a cuáles son realmente las dudas o recelos que suelen embargar a cualquier usuario cuando se le plantea la posibilidad de realizar una transacción digital (en el más amplio de los sentidos) en Internet. Tales recelos son los que, mediante un conjunto apropiado de servicios, el sustituto electrónico del notario humano debería ayudar a evitar. La segunda cuestión se refiere a qué otros esquemas y soluciones relacionadas han sido planteadas hasta el momento, y así estudiar cuáles han sido las ventajas e inconvenientes de cada una de ellas.

Respecto a la primera cuestión, entre las muchas dudas que surgen en los diversos escenarios que se pueden dar, quizá podrían resaltarse las siguientes:

- ¿Es la entidad con la que estoy contactando real, o ficticia?

- ¿Habrá modificado alguien el contenido de la transacción?
- ¿Se habrá recibido la transacción a tiempo en destino?
- ¿Estará de acuerdo el destinatario con el contenido?
- ¿Y si el destinatario niega haberla recibido (toda o parte)?
- ¿Y si niega haber intervenido, o incluso no conocerme?
- ¿Quién me notifica a mí la recepción?
- ¿Cómo me aseguro de que no utilizará "incorrectamente" esa información que se supone confidencial?
- etc.

Respecto a la segunda cuestión, se pueden considerar varios esquemas que, tanto por su nombre como por su intención, quedan muy cercanos al objeto de análisis de este artículo. A continuación se revisan someramente tres ejemplos que merecen un especial interés.

Servicio de Notarización Digital (Surety Technology)

Surety Technology es una empresa americana creada en 1994 para explotar comercialmente una idea relacionada con el estampillado digital de tiempo sobre documentos en formato electrónico [4]. Ya entonces, esta compañía estimó que debido al incipiente uso de medios electrónicos por parte de las empresas, y consecuentemente de documentos digitales, resultaba esencial desarrollar un método seguro de precintado individualmente cada uno de ellos. De la misma forma, consideraron necesario proporcionar un método irrefutable para verificar que un documento había sido creado en un momento determinado y que no había sido alterado con posterioridad.

Así, su Servicio de Notarización Digital utiliza un sistema criptográficamente seguro para el precintado de documentos y es aplicable a cualquier tipo de fichero. Este sistema de autenticación documental opera de forma independiente a la seguridad del sistema, garantizando, en primer lugar, que el documento ha sido creado en un día y hora específicos; en segundo lugar, que el documento no ha sido alterado desde esa fecha; y, por último, que no puede ser confundido con ningún otro documento.

Una peculiaridad del sistema es que no se utilizan claves, pues la formulación matemática construida dentro del Servicio se basa en la utilización de funciones resumen unidireccionales, mediante las cuales se crean huellas digitales únicas para cada documento. Funciona en modo cliente/servidor, de tal forma que el software ejecutado en la parte del cliente crea la huella digital, que es transmitida al Servidor de Notarización de Surety. De este modo, el documento original nunca sale de la empresa propietaria, y nadie más que su legítimo dueño tiene acceso a él. El Servidor de Notarización devuelve un registro notarial (con efecto de certificado electrónico) que precinta el contenido del documento. El registro contiene toda la información necesaria (incluyendo la fecha y hora de la certificación) para que el documento pueda ser validado en un futuro.

Internamente, el Servidor recibe peticiones de certificación de muchas compañías diferentes en intervalos de 1 segundo. Esas peticiones incluyen, cada una, el valor resumen de un documento. Los valores resúmenes se enlazan para construir un árbol ascendente, como muestra el ejemplo de la figura 1. De esta forma, todas las certificaciones realizadas por Surety en su historia quedan concentradas en un único valor, y cada uno de los valores recibidos depende de todos los demás, con lo que la robustez del sistema queda garantizada.

Autoridad Notarial (IETF)

El grupo de trabajo PKIX de la Internet Engineering Task Force (IETF) propuso a principios de 1997, dentro del trabajo de desarrollo de una PKI, la creación de una entidad digital denominada Autoridad Notarial [5]. Esta Autoridad es una parte confiable que verifica la corrección de unos datos específicos que se le envían, proporcionando el por ellos denominado servicio de notarización, con el objeto de construir evidencias de no-repudio relativas a: (1) la validez y la corrección de la demanda de un usuario respecto a la posesión de unos datos; (2) la validez y el estado de revocación de un certificado de clave pública; y (3) la validez y corrección de una firma digital.

Cuando la Autoridad notariza la posesión de unos datos, o la

firma realizada por alguna entidad, simplemente verifica la corrección matemática del valor de la firma contenida en la petición, y chequea, además, el camino de certificación, contactando con las Autoridades de Certificación (CAs) pertinentes. La Autoridad Notarial ha de ser capaz de acceder a las Listas de Revocación de Certificados, o incluso de utilizar algún medio adicional para conseguir el estado más actualizado posible.

Por otro lado, cuando notariza un certificado, verifica que éste es válido y determina el estado de revocación a la hora especificada. También en este caso chequea el camino de certificación.

Tanto en uno como en otro caso la Autoridad Notarial emite tokens notariales, que llevan incluida una estampilla digital de tiempo, y son utilizados por los propios usuarios con posterioridad para autenticar la posesión y la corrección de los correspondientes datos.

CiberNotarios (ABA)

Esta iniciativa surgió a finales de 1997 en el núcleo de la Asociación de Colegios de Abogados de Estados Unidos (ABA - American Bar Association). La sección de Ciencia y Tecnología de esta Asociación vislumbraba entonces que la aparición de cierto tipo de comercio electrónico internacional iba a exacerbar, en gran medida, un hecho ya conocido: el impedimento para hacer respetar los actos legales de los EE.UU. fuera de sus fronteras.

Tradicionalmente, las diferencias entre los distintos países en cuanto a los requisitos, tanto de contenido como de procedimiento, para muchos tipos de transacciones internacionales, han dado como resultado el rechazo de numerosos documentos norteamericanos por parte de las autoridades legales de otros países. Este hecho ha sido particularmente obvio en países cuyos sistemas legales derivan de la ley civil romano-germánica, pero también existen problemas con otros países con los que Estados Unidos comparte una ley más o menos común, incluyendo a Gran Bretaña y a Suráfrica.

Por ello, el grupo antes mencionado ha considerado la necesidad de la existencia de algún tipo de autenticación de alto nivel, así como la adecuada certificación de documentos electrónicos que aseguren la fiabilidad y el cumplimiento de los actos subyacentes. La solución planteada ha sido la creación de un nuevo profesional legal, el CiberNotario, cuyo papel combina de forma complementaria la experiencia técnica con la legal en una sola especialización.

La primera de las funciones en Estados Unidos de un CiberNotario es similar a la actualmente desarrollada por los notarios latinos. Con ello se persigue que cualquier CiberNotario garantice que sus actos tengan efecto en jurisdicciones extranjeras.

La segunda función es la de poseer capacidades de certificación y autenticación extendidas; es decir, no sólo ha de dar fe sobre documentos en papel, sino también sobre documentos en formato digital. Esto obliga a que los CiberNotarios posean un alto nivel de cualificación en la tecnología de Seguridad de la Información. De hecho, el proyecto plantea la posibilidad de que actúen como Autoridades de Registro de CAs externas a ellos, con la función de verificar las identidades de los usuarios y certificar, no sus claves públicas, sino las peticiones que se envían a las CAs solicitando la emisión de los certificados de clave pública.

IDENTIFICACIÓN DE LOS SERVICIOS

Un rápido análisis de estos tres esquemas pone de manifiesto algunos inconvenientes. La solución de Surety, aunque robusta, no pasa de ser un sistema de estampillado digital de tiempo, siendo evidente que con esto no se resuelven todas las preguntas que habíamos planteado con anterioridad y que un notario electrónico debería de satisfacer a través de sus servicios. De la misma forma, la solución del PKIX es sólo un sistema de estampillado, y su futuro inmediato es incierto porque ni siquiera ha alcanzado el nivel de RFC (Request for Comment) en la IETF. De hecho, existen discrepancias en el grupo de trabajo sobre la denominación exacta que este esquema ha de recibir, de tal forma que en 1998 pasó a denominarse Servidor de Certificación de Datos, y en 1999, Servidor de Certificación y Validación de Datos [6]. Respecto a la propuesta de la ABA, además de que el proyecto ha sido paralizado por cuestiones de

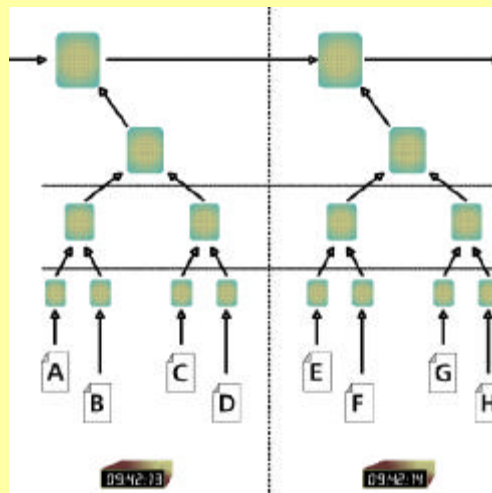


Figura 1

indole legal, es obvio que al ser el CiberNotario una figura humana se aleja un tanto de ese mecanismo digital buscado y necesitado para el comercio electrónico.

Sin embargo, el estudio de este último esquema pone claramente de manifiesto un problema generalizado en estas tres soluciones, y en algunas otras que han seguido unas pautas similares. Nos referimos al hecho de que toman al notario anglosajón como referencia. La labor primordial de éste es dar autenticidad a las firmas que se realizan en un documento, pero no a su contenido, de tal forma que identifica a los firmantes y solamente certifica que éstos firman el documento en su presencia en ese día y hora. Parece claro pues que tomando como referencia a este tipo de notario no se van a poder construir los servicios necesarios para el comercio electrónico.

Por el contrario, si resulta mucho más factible si la referencia a seguir es la del notario latino, cuyas funciones, más numerosas y complejas que las del notario anglosajón, son de sobra conocidas por todos nosotros. De hecho, la formulación adecuada de los servicios mencionados pasaría por dar una respuesta directa al conjunto de preguntas anteriormente planteadas, pero tomando como referente los servicios tradicionalmente prestados de los notarios latinos, y teniendo en cuenta la diferencia de matices entre el escenario digital y el del basado en soporte papel.

Siguiendo este criterio, puede realizarse una primera aproximación al conjunto de operaciones que ha de llevar a cabo el notario electrónico para garantizar seguridad y fiabilidad a las transacciones digitales. Entre estas operaciones destacan: autenticar a las partes, fechar documentos digitales, detectar la falsificación o manipulación de mensajes por parte de usuarios no honrados, confirmar que los usuarios reciben los mensajes adecuados en los momentos apropiados, e incluso almacenar las evidencias y registrar los accesos.

A partir de aquí se pueden establecer los siguientes servicios:

- Autenticación de entidades
- Certificación de fecha y hora
- Certificación de envío
- Certificación de entrega
- Certificación de contenidos
- Soporte de confidencialidad
- Salvaguarda de datos digitales
- Registro de accesos y procesos

A continuación se revisan aquellas funciones de la lista anterior que tienen una relación más directa con la Seguridad de la Información, con el objeto de ofrecer una breve pincelada de las implicaciones que conllevan.

La autenticación de entidades es, sin duda, una función muy importante dentro un servicio de notaría electrónica. Resulta esencial que, antes de iniciar una determinada operación, cualquier usuario involucrado en la transacción tenga plenas garantías sobre la autenticidad de la(s) entidad(es) con la que va a establecer la comunicación, así como de la autenticidad de los documentos firmados por ésta(s). Además, ha de tener la certeza de que cualquier entidad electrónica remota posee no sólo una identidad electrónica veraz, sino también una identidad física en el mundo real que se corresponde de forma unívoca con la electrónica.

Con bastante frecuencia los términos "identificación" y "autenticación" han sido utilizados indistintamente para hacer referencia a todo el complicado proceso relacionado con cómo garantizar a un usuario que otro usuario con el que va a establecer la comunicación es quien dice ser. Tal confusión en la utilización de ambos términos es debida a la estrecha relación que existe entre ellos. Con la autenticación se pretende, ante todo, confirmar la identidad de un usuario que ha sido registrado anteriormente. Precisamente, será labor preliminar del notario electrónico identificar de forma correcta (directamente, o indirectamente apoyándose en Autoridades de Registro), a cualquier entidad que pase a formar parte del sistema, y habrá de crear pruebas de su registro. Estas pruebas serán usadas por el resto de usuarios para autenticar al primero.

Existen distintos tipos de pruebas y, por tanto, diferentes métodos o modelos de autenticación. Los modelos basados en factores biométricos, contraseñas, y posesión de tokens son útiles para sistemas en los que el número de usuarios no es elevado y en los que la dispersión geográfica de los usuarios es moderada, pero en ningún caso están indicados para aplicaciones globales, como es el caso de las aplicaciones de comercio electrónico. Sin duda, el modelo de autenticación basado en certificados digitales, ampliamente comentado en números anteriores de esta revista, es el ideal para escenarios globales. Esto significa que los notarios deberían asumir las funciones tradicionalmente llevadas a cabo por las Autoridades de Certificación, y, de cierto modo, los notarios podrían ser considerados como macro-Autoridades.

Respecto a la certificación de fecha y hora, y de la misma forma

que ocurre en los procedimientos administrativos basados en soporte papel, está clara la necesidad de poder conocer y demostrar fehacientemente que un hecho (generación, intercambio, firma, etc. de un documento digital) ocurrió en un determinado instante de tiempo, así como de poder relacionarlo cardinal y ordinalmente frente a otros hechos.

Sin embargo, la versión digital de tal certificación presenta un problema: la inmaterialidad del documento. El uso amplio de documentos electrónicos representa una seria amenaza a la viabilidad de los procesos de fechado y la fácil modificación de un documento digital, junto a la ausencia de marcas que prueben que ha sido modificado, hacen surgir dudas justificadas sobre cualquier afirmación relativa a la fecha de creación o modificación de tal documento. Queda claro, por lo tanto, la necesidad de utilizar un sistema o servicio de fechado de documentos digitales, quitándole al autor del documento la posibilidad de producir una fecha distinta de la real, y transfiriendo el control del proceso de fechado a una tercera parte independiente y confiable.

Aunque tradicionalmente han sido las autoridades de fechado (TSAs) las encargadas de esta labor, la integración de este servicio como una de las funciones del notario electrónico nos parece la forma más razonable, apropiada y eficiente de certificar documentos que vayan acompañados de su correspondiente estampilla de tiempo, sin necesidad de tener que acudir a entidades externas que realicen ese fechado. Esta solución ofrece interesantes ventajas porque muchos de los documentos digitales a fechar han de ser generados por el propio notario, evitándose con ello la obligación de utilizar protocolos específicos para comunicarse con las TSAs. La ventaja es mayor aún si se considera que la incorporación de cualquier protocolo complejo de seguridad no hace sino abrir una posible puerta a los ataques externos, habida cuenta de que las técnicas de análisis y diseño de tales protocolos están aún en una fase muy temprana de investigación y resultando altamente difícil garantizar al ciento por ciento que no tiene fallos [7].

Las certificaciones de envío, entrega y contenidos resultan elementos fundamentales a la hora de dotar de fiabilidad a las típicas transacciones de comercio electrónico. Hasta hace poco estos factores no habían sido especialmente estudiados en el campo de la Seguridad de la Información porque siempre había estado subyacente la idea de que las mayores amenazas podían venir de terceras partes no implicadas en la comunicación. No obstante han sido especialmente las aplicaciones de comercio electrónico las que han puesto de manifiesto el hecho de que muchas veces "el enemigo se encuentra en casa". La experiencia viene a demostrar la amenaza de que cualquiera de las partes supuestamente honradas involucradas en la propia transacción puede tener un comportamiento fraudulento, negando, por ejemplo, el envío o la recepción de un mensaje o de un documento. El hecho de que las entidades estén distribuidas en distintos lugares y bajo normativas distintas, además, de que las transacciones no se realizan en persona y de que en ningún caso hay evidencia física de la transacción, agravan más si cabe el problema.

Poder enlazar la autenticación de las acciones con las entidades que intervienen en la comunicación, así como vincular la responsabilidad del autor a lo que hace, resulta esencial [8]. El servicio de no-repudio es el procedimiento que protege a cualesquiera de las partes involucradas en una comunicación de que alguna de las otras tenga éxito cuando niegue ilegítimamente que un determinado evento o acción haya tenido lugar. Este servicio ha de producir, validar, mantener y poner a disposición de las partes, pruebas o evidencias irrefutables respecto a la transferencia de información desde un origen a un destino, así como de la recepción y el contenido de la misma.

El servicio de no-repudio está íntimamente relacionado con el de autenticación, pero el primero tiene que cumplir más requisitos que el segundo en cuanto a las pruebas que ha de producir. La diferencia básica 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 autenticidad, mientras que el no-repudio, además, ha de probar esas mismas cualidades ante otros que no participan en la comunicación. Se puede entrever que va a ser necesaria la intervención, en mayor o menor medida, de una tercera parte en la que los usuarios confíen, pues partimos de la base de que entre ellos tal confianza no es absoluta. Las partes necesitan obtener suficientes evidencias para resolver sus diferencias, bien entre ellas mismas, o bien utilizando algún tipo de arbitraje, y no cabe duda de que el notario electrónico es la figura digital más apropiada.

Por lo tanto, el notario electrónico va a intervenir, de una u otra forma, en la ejecución de cualquier protocolo de no-repudio. Las pautas de actuación del notario variarán dependiendo de la política de no-repudio, de los mecanismos utilizados y, sobre todo, de las necesidades de los usuarios. Así, se pueden definir básicamente dos

tipos de intervención. En la intervención interactiva el notario tomará un papel predominante, y habrá de proporcionar las evidencias que los usuarios necesitan, o bien verificará la corrección de las evidencias producidas durante la transacción, o bien se limitará a entregar certificados de mensajes entre las entidades. Por el contrario, en la intervención diferida no se implicará en el servicio de no-repudio a menos que exista un problema que resolver y se precise de un arbitraje imparcial, por lo que su papel será más pasivo. En este caso se limitará a resolver disputas, cuando éstas se planteen, sobre la ocurrencia o no de un determinado evento.

La diferencia entre ambos tipos de actuación queda patente al observar los flujos de comunicación de dos protocolos tipo (figura 2). En el primero todos los flujos pasan a través del notario, mientras que en el segundo el notario sólo interviene (líneas discontinuas) si el protocolo no se desarrolla por los cauces normales. Serán los usuarios los que decidan la implicación directa del notario por, por ejemplo, estar involucradas cantidades económicas elevadas en la transacción. Es obvio, que en el primero de los casos los usuarios tendrán que pagar una tarifa mayor que en el segundo por la intervención del notario.

Por último, y respecto al soporte de confidencialidad, es necesario precisar que, en primer lugar, dentro del conjunto de transacciones comerciales va a existir la necesidad de que algunos flujos de información, especialmente aquellos relativos a mensajes o documentos a compartir o intercambiar entre los notarios electrónicos, sean especialmente confidenciales. En segundo lugar, el conjunto de notarios dentro de una infraestructura puede estar, en principio, perfectamente definido. Ambos puntos llevan a pensar en la conveniencia de configurar un esquema de Red Virtual Privada (RPV) entre los notarios de la infraestructura.

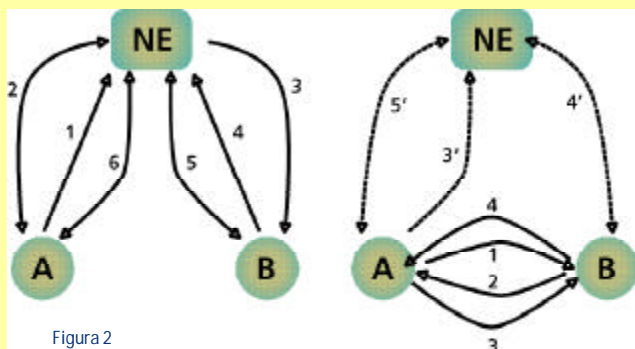


Figura 2

Sin embargo, un estudio de las distintas capas de la torre de protocolos de TCP/IP pone de manifiesto que las soluciones ya desarrolladas para permitir el establecimiento de RPVs se preocupan, esencialmente, de los aspectos de seguridad. En ellas, los principales objetivos son aislar una red distribuida y proteger la privacidad y la integridad de la información sensible que pasa a través de Internet. El gran inconveniente de establecer el problema de la seguridad como objetivo principal es que los usuarios de la RPV sufren restricciones en el acceso a Internet. Es decir, no pueden mantener el uso libre de los servicios tradicionales, y en este caso eso es necesario para los notarios electrónicos.

Realmente, es necesario permitir el acceso genérico de los usuarios de la RPV a Internet y, simultáneamente, mantener un modelo de seguridad con suficientes garantías. Esto no resulta ni mucho menos fácil ya que, por lo anterior, resultará recomendable que el esquema posea ciertas características, como: (a) ser una solución exclusivamente software; (b) facilitar la utilización de los servicios tradicionales de Internet sin necesidad de modificar las aplicaciones tradicionalmente inseguras; (c) permitir a los notarios decidir en qué situaciones aplicar los mecanismos de seguridad; (d) posibilitar la conexión tanto a otros notarios de la propia red como a usuarios que no pertenecen a ella.

Todos estos servicios de los notarios electrónicos, incluidos aquellos que no están directamente relacionados con la seguridad, quedan representados en la figura 3. Se puede observar que en el centro de la figura aparecen aquellos servicios propios de las Autoridades de Certificación, que como ya se comentó anteriormente, deberían ser adoptados por los notarios electrónicos.

CONCLUSIONES

El papel de los notarios electrónicos, así como el de los servicios digitales proporcionados por éstos, va a resultar fundamental en la implantación del comercio-e a escala global, y debe venir facilitado por la familiaridad que entre todos nosotros tiene la intervención de su homólogo humano en muchos de los procedimientos administrativos basados en soporte papel. No cabe duda de que las empresas que desarrollan productos de seguridad habrán de incorporar en ellos, y a corto plazo, tales servicios como elementos diferenciadores. De la misma forma, las empresas que proporcionan servicios de seguridad habrán de proporcionar a sus clientes los nuevos servicios de notarización, pues éstos y las infraestructuras de notarios electrónicos no son más que el siguiente paso natural a los servicios de certificación y las PKIs. Sin embargo, y respecto a los servicios a proporcionar por estos nuevos agentes digitales, aún queda mucho por hacer.

En este artículo se han revisado algunas propuestas relacionadas, y se ha llevado a cabo una breve descripción de las funciones que deberían integrarse en un notario electrónico. Estas funciones no son del todo desconocidas, pero han de evolucionar convenientemente. Por ejemplo, aunque los notarios electrónicos pueden ser las entidades más adecuadas para la emisión de los tan nombrados certificados de atributo, parece claro que no es el estándar X.509 la mejor solución, porque no fue diseñado para ello. Sin duda, hacen falta nuevas propuestas.

Por otro lado, los protocolos de no-repudio están sólo en una primera fase porque no se ha investigado el diseño de los mismos en escenarios multiparte, esenciales en el comercio electrónico. También, los servicios cooperativos de estampillado digital son casi inexistentes, funcionando en su mayoría como islas. La introducción de esta función en los notarios digitales requiere de tal cooperación. Por último, cabe hacer notar que hasta el momento se ha prestado mucha mayor atención a las soluciones de seguridad para servicios basados en TCP que a los de UDP, y hay que tener en cuenta que tanto el audio como el video serán elementos esenciales en el verdadero comercio electrónico que está por llegar. n



Figura 3



2 Javier López Muñoz
E.T.S. Ingeniería Informática
UNIVERSIDAD DE MÁLAGA
jlm@cc.uma.es

REFERENCIAS

- [1] Directiva relativa a determinados Aspectos Jurídicos del Comercio Electrónico (Mercado Interior), Comisión Europea, febrero 2000.
- [2] "Anteproyecto de Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico", Ministerio de Ciencia y Tecnología, enero 2001.
- [3] Jefatura del Estado, "Real Decreto-ley 14/1999, de 17 de septiembre, sobre Firma Electrónica", Boletín Oficial del Estado, 21-septiembre-1999.
- [4] S. Haber, S. Stornetta, "How to Timestamp a Digital Document", Journal of Cryptology, v.3, 1991, pp. 99-111.
- [5] C. Adams, R. Zuccherato, "Internet X.509 Public Key Infrastructure. Notary Protocols", PKI Working Group, Internet-Draft, febrero 1997.
- [6] C.Adams, A. Sylvester, S. Zolotarev, R. Zuccherato, "Internet X.509 Public Key Infrastructure. Data Validation and Certification Server Protocols", PKIX Working Group, Internet-Draft, octubre 1999.
- [7] S. Gürgens, J. López, R. Peralta, "Efficient Detection of Failure Modes in Electronic Commerce Protocols" IEEE International Workshop on Electronic Commerce and Security, septiembre 1999, pp. 50-57.
- [8] J. A. Mañas, "Transacciones de Comercio Electrónico con Garantía Técnica de Prueba", Securmática, abril 2000.