



LA NOTIFICACIÓN DIGITAL HACIA LOS CIUDADANOS: CARACTERÍSTICAS Y POSIBLES MODELOS

El de las PKI's y lo que con ellas se puede hacer, es uno de los temas más actuales y manidos del sector profesional relacionado con la seguridad informática; sin embargo, aún le queda mucho por madurar. Quizá la emisión de certificados ya sea un aspecto bastante agotado de esas tecnologías, pero hay

todavía asuntos y funcionalidades que no se han tratado suficientemente en serio y son componentes críticos en cuanto a la posible utilidad real del sistema.

Una de estas cualidades deseables sería la de poder realizar entregas y notificaciones certificadas entre distintos agentes de la red. En particular lo que más nos interesa ahora tratar es la posibilidad de poder entregar información hacia el ciudadano y hacerlo de modo confidencial, autenticado y con **carácter de no repudio en cuanto a la recepción** del documento.

De existir realmente esa posibilidad, podrían desaparecer las miles de notificaciones en papel que hoy son la base de muchos procesos administrativos públicos y privados. Podrían, por ejemplo, desaparecer las notificaciones que nos informan de los movimientos que sufren nuestras cuentas bancarias, las citaciones de la administración no tendrían por qué suponer una caminata del cartero hasta nuestras casas—casi siempre vacías—, y que ese envío se convierta, al final, en un paseo nuestro hasta la correspondiente Agencia de Correos. Con un sistema de entrega o notificación certificada, el ciudadano también podría enviar a la Administración sus declaraciones y oficios, pudiéndose quedar tranquilo y seguro de que aquella las recibió y nunca podrá decir lo contrario, etc.

Son muchas las ventajas imaginables en el caso en el que se pueda obtener la certificación de la entrega de información digital y sin embargo, no es un tema al que se le esté haciendo mucho caso en el mundo empresarial.

Hace ya varios años, una curiosa iniciativa¹ de Bancos y Cajas de Ahorro dio como resultado el programa de contabilidad doméstica Efectivo98², que permi-

Supongamos que el mundo de las PKIs ya fuese una realidad y no una eterna promesa, y que cada uno de los ciudadanos dispusiese de una o varias identidades digitales que le permitiesen disfrutar de sus derechos y atender a sus obligaciones. En este escenario, los ciudadanos podrían dirigirse, a través de redes como Internet, a la Administración, instituciones financieras, bancos, y entidades de todo tipo. Sin embargo, ¿qué pasa con la comunicación en el otro sentido? ¿Puede, por ejemplo, la Administración ponerse en contacto con un ciudadano y estar segura de que éste recibirá su mensaje? ¿Es posible eso incluso cuando el ciudadano encuentre algún beneficio es negar tal recepción?

tía al usuario un conocimiento actualizado de sus gastos personales, recibos y domiciliaciones. Este programa permitía conectarse con los bancos a través de Internet para recoger información sobre movimientos y actualizar las cuentas de cada cliente hasta el último apunte disponible. La aplicación Efectivo98 fue desarrollada para ejecutarse en máquinas con Windows 95/98 y también funciona en NT, pero no lo hace en Windows 2000; lo cual no es un indicio muy prometedor en lo que a la continuidad de esta idea se refiere.

En alusión a la información que contiene, este servicio es equivalente a las notificaciones bancarias en papel que periódicamente llegan a nuestros buzones. En ningún caso, el uso de ese servicio suponía el cese de las notificaciones «clásicas» en papel porque, a fin de cuentas, lo que valía legalmente es el envío por correo de esos mismos apuntes convenientemente impresos por la entidad bancaria en su papel de aguas. La única manera que tenía el banco de saber que había llegado esa información a su cliente era enviársela por correo ordinario o, directamente, dejársela en el buzón de su casa.

A cualquiera le resulta obvio que en el mundo digital es necesario conseguir, al menos, los mismos niveles de «irreversibilidad» y publicidad parcial que encontramos en la vida cotidiana plagada de documentos en papel. Si alguien se presenta a un examen y le hacen entrega del enunciado de los ejercicios, nunca se atreverá a alegar que no pudo contestar correctamente «por desconocer las preguntas planteadas». Todos los testigos presentes en aquel instante y lugar, podrían declarar que se le entregó la misma documentación que a todos los demás y que,

entonces, no presentó públicamente ninguna queja, por lo que estaba aceptando implícitamente que todo ocurría según lo que es normal en estas circunstancias.

Lo mismo sucede cuando un cartero entrega una carta certificada y la aceptamos; en el caso de disputas posteriores, sin duda

testificará y al ser independiente de lo contenido en el envío, su declaración será tomada muy en cuenta. Si intentamos repetir ese mismo proceso de modo no presencial, desaparecen la multitud de testigos que podrían declarar qué es lo que realmente ocurrió. En un escenario telemático, la «realidad» sólo tiene uno o, a lo sumo, dos personajes involucrados, por lo que recurrir a las declaraciones de testigos casuales es, hoy por hoy, imposible.


Este tipo de problemas se intentan solucionar con lo que se denominan, de una forma muy genérica y un tanto pomposa, «Terceras Partes Confiables» (TPCs), cuya misión esencial sería actuar como testigos en ese tipo de situaciones³. La opción más ingenua para conseguir un cierto tipo de «entrega certificada» de una información digital es la de proponer que el remitente se la envíe a la TPC y que el destinatario tenga que ponerse en contacto con ella para recibir dicha información. Sin embargo, esta solución no es, de ningún modo, aceptable.

Un sistema de entrega certificada debe respetar la confidencialidad y el derecho a la intimidad de los comunicantes. Más aún, la participación de esas entidades debería ser absolutamente «ciega» y desconocerlo todo sobre la información que ayudan a entregar ya que, de lo contrario, se convertirían en unos puntos de acumulación de informaciones muy variadas y, por tanto, en uno de los objetivos más claros de piratas, agentes de la seguridad nacional, espías, compañías de marketing, etc.; lo que haría mucho más difícil y cara su defensa. Además de esto, dichas

¹ IPI = Informática Personal Interbancaria

² <http://www.efectivo98.com/efectivo/indexnet.htm>

³ ver « DISEÑO DE PROTOCOLOS DE NO-REPUDIO » Ágora, Revista SIC Nº 38 (febrero de 2000)



Agencias podrían dejar de ser «imparciales» y eso daría al traste con su reputación (= confianza).

Esta operación de asistencia al envío y a la entrega de un objeto digital debe estar adecuadamente referida en la escala del tiempo; no sólo es importante que las cosas lleguen a su destino, sino también cuándo lo hacen. Cualquier infraestructura de entrega certificada deberá hacer un uso extensivo de los servicios de sellado digital de tiempos que le permitan demostrar ante cualquiera en qué momento se produjeron los hechos; de este modo queda perfectamente descrito el hecho de la entrega, único aspecto que debe preocuparle.

El que en la recepción y entrega de la información la TPC deba ser absolutamente ciega, no quiere decir que los agentes involucrados en la transferencia no deban estar perfectamente identificados los unos ante los otros. Los sistemas de certificación de entrega son servicios avanzados de seguridad que se construyen sobre una constelación de PKIs adecuadamente instaladas y gestionadas.

Otro de los problemas que presenta la entrega certificada es ¿dónde localizar al destinatario? Debido a la volatilidad del

mercado y mundillo de los ISPs, lo normal es que los ciudadanos, en general, no dispongan de un servicio de correo electrónico de calidad, y tienden a tener varias cuentas de correo que no consultan sistemáticamente. El resultado de todo ello es que uno nunca puede saber, a fe cierta, si la dirección a la que hace el envío es, en ese momento, de las «activas» para ese destinatario. La falta de unicidad en

El problema de la entrega certificada de información digital es uno de los temas clave para poder construir, de manera sólida, una sociedad basada en las Tecnologías de la Información.

las cuentas de correo es equivalente al caso en el que cada ciudadano pudiese tener varios domicilios y no supiésemos realmente dónde vive.

Aunque las modernas redes de comunicación permiten cada vez más la movilidad espacial de los usuarios, no por ello deja de ser necesario que siga habiendo cosas que no cambian, y es necesario construir en ese nuevo medio el equivalen-

te digital a la «dirección postal» oficial de un individuo que aparece en censos tan universales como el electoral o el padrón.

El problema de la entrega certificada de información digital es uno de los temas clave para poder construir, de manera sólida, una sociedad basada en las Tecnologías de la Información. El concepto de las Terceras Partes Confiables, la asistencia ciega a la entrega, la referencia temporal de las fases de la entrega mediante sellos de tiempo, la identificación de los agentes a través de PKIs, etc., son cosas ya disponibles por lo que nada parece impedir que se ofrezcan servicios de certificación de entrega; sin embargo, este asunto sigue siendo un problema abierto que no están sabiendo resolver correctamente las empresas. Me consta que en el mundo universitario estos temas ya son conocidos desde hace tiempo y quizá sea por ese lado de donde terminen llegando las soluciones. Por el momento, habrá que esperar y seguir despilfarrando toneladas de papel. ●

JORGE DAVILA MURO
Laboratorio de Criptografía
LSIIS - Facultad de Informática - UPM
jdavila@fi.upm.es