



e-Government: ¿qué falta?

La campaña de declaraciones IRPF y Patrimonio 2000 de este año parece haber sido un verdadero éxito. Con anterioridad al 20 de junio, plazo para la entrega de las declaraciones positivas, la Agencia Tributaria había recibido 380.873 declaraciones a través de Internet¹, lo que supone tres veces más que en la campaña anterior, donde fueron 115.244 las presentadas² por ese sistema, según datos de la Fábrica Nacional de Moneda y Timbre.

La conveniencia del sistema para el ciudadano es clara; el 50% de las presentaciones telemáticas se hicieron en horario de tarde o noche y el 10,5 % se realiza durante los fines de semana, en ambos casos la administración física tradicional está cerrada a «cal y canto». Además de poder realizar las operaciones cuando al contribuyente le viene bien, el sistema telemático elimina, o al menos disimula, la necesidad de tener que hacer colas para cumplir con el erario público.

En cuanto al número de diferentes agentes que ya están acreditados ante la Administración tributaria para estos fines, el número de certificados ha pasado de ser 17.566 en la campaña de 1999 a 61.015 en la del 2000 lo que supone un crecimiento del 347 por ciento.

Todo esto está muy bien pero en esta campaña se ha incluido un nuevo servicio de la AEAT: la emisión de certificaciones de haber presentado la declaración mediante estos avanzados sistemas que aporta Internet. Siendo un usuario convenientemente registrado a través del correspondiente certificado, podemos solicitar que se nos certifique que hemos presentado nuestra declaración del IRPF. La solicitud³ se hace a través de la web de la Agencia y, curiosamente, te dicen que «*estará disponible en la opción de Recogida transcurridos dos días laborables.*»⁴

Los certificados se recogen también a través de la web⁵, y lo que uno se encuentra cuando lo hace es un formu-

La necesidad de disponer –por parte de las administraciones– de sistemas de notificación y entrega a los ciudadanos de documentos electrónicos oficiales es un elemento fundamental para el funcionamiento del denominado e-Government. Para ello resulta necesario dotarse de una infraestructura que satisfaga ciertos principios y en la que, además de poder asignar al receptor un ‘apartado de correo-e’, puedan intervenir, entre otras y de forma independiente, una autoridad de sellado temporal y un ‘notario ciego’ a efectos de conseguir el no-repudio. El modelo se presenta como una alternativa que resuelve el problema de la entrega certificada de objetos digitales.

lario en HTML que puede imprimir y en el que se indican los datos de la «etiqueta» del contribuyente y la constancia de haber presentado la declaración correspondiente, la fecha y hora a la que se emite el mencionado certificado y un «Código Seguro de Verificación de la Expedición» seguido de una sobrecogedora secuencia de ocho bytes en hexadecimal y eso es todo.

Una posible solución sería que el Estado Español proporcionara los medios necesarios para que todos los contribuyentes pudiesen tener cuentas de correo electrónico que actuasen como los «apartados de correos» clásicos en los que recibir los mensajes oficiales en general

¿Cómo es posible? ¿No tenemos perfectamente identificados a los contribuyentes? ¿No conocemos todos al servidor de la Agencia Tributaria⁶? Entonces, ¿por qué no va firmado el mencionado certificado HTML? ¿De que me sirve un sigiloso número en hexadecimal que no entiendo? ¿Cómo puedo comprobar que lo que imprimo o guardo es realmente un documento firmado por la AEAT y que, en el futuro, me puede defender de falsas acusaciones por parte de ésta?

Mientras que las declaraciones van adecuadamente firmadas por el ciudadano, las respuestas de la Administración llevan una especie de código autenticador de mensajes (MAC) que sólo ellos saben generar y verificar, convirtiéndose, de este modo, en «juez y parte» en el caso de que la AEAT termine solicitando pruebas de haber presentado la declaración. ¿Por qué la Administración Espa-

ñola no se atreve a firmar digitalmente? No lo sé.

SISTEMAS DE NOTIFICACIÓN Y ENTREGA CERTIFICADA DE DOCUMENTOS

El hecho de que se haya puesto en marcha tímidamente este servicio pone de manifiesto que el denominado e-Government necesita de sistemas de notificación y

entrega certificada de documentos para poder funcionar.

Los elementos y tesis básicas que describen a estos sistemas son:

1. Todos los agentes deben estar convenientemente identificados y entre ellos deben existir vínculos de confianza, libremente asumidos, que permitan la aceptación mutua de identidades.
2. Todos los prestadores de algún tipo de servicio a la comunidad de usuarios deben tener públicamente definida y accesible su «deontología» en forma de un documento en el que se defina su política de actuación, los procedimientos que sigue y, en su caso, las responsabilidades que asume en el ejercicio de sus actividades.
3. Debe haber autómatas que actúen como «Notarios Ciegos» que participen en cada entrega o transferencia documental entre el destinatario y remitente de un envío digital, aportando su testimonio independiente para obtener el no-repudio de la transacción.

1 Esta cifra representa un 7,4% del total de declaraciones.
 2 Esta cifra sólo supone el 1% del total de todas declaraciones presentadas en la campaña del IRPF 1999
 3 <https://aeat.es:8002/renta2000/certrena.html>
 4 Hasta en la versión telemática de la AEAT sigue siendo válido eso de ¡vuelva usted mañana! ¡Los hay que no aprenderán nunca!
 5 <https://aeat.es:8002/renta2000/certrenc.html>
 6 De esto habría que hablar con mas calma pero este no es el momento.

4. El *Notario Ciego* no debe conocer nada acerca del contenido del objeto digital transferido y tampoco debe tener acceso a éste en ninguna de sus formas.

La necesaria independencia del notario o agente de entrega debe basarse en la imposibilidad de que éste pueda llegar a ser parte, directa e indirectamente, en la transferencia de la información como tal. Dicho de otro modo, el notario debe saber y dar fe de que se ha realizado una transacción entre remitente y destinatario, pero debe ser incapaz de identificar, a partir de lo que conoce, cuál fue el contenido de lo transferido.

5. La transferencia de los objetos digitales entre origen y destino debe realizarse a través de un sistema no relacionado con los agentes que actúan como fedatarios de entrega.

La entrega del objeto digital protegido⁷ debe ser previa a la notarización propiamente dicha y puede hacerse o bien directamente entre remitente y destinatario a través de sistemas asíncronos e intermediados como es el caso del correo electrónico, o mediante conexión directa entre ellos. La transferencia puede ser confidencial o no, dependiendo de cual sea el mecanismo elegido pero, en cualquier caso, no necesita ser autenticada ya que esa cualidad le vendrá dada por la intervención del *notario ciego*.

6. Una vez realizada la entrega, destinatario y remitente deben disponer de exactamente la misma información y pruebas de la transferencia, y la verificación de su autenticidad debe hacerse con absoluta independencia del agente fedatario que participó en su generación. Este principio de equi-

librio y medida es necesario para asegurar la legalidad, credibilidad y aceptabilidad del sistema.

7. Las operaciones que componen los protocolos de notarización deben estar marcadas cronométricamente con Sellos Digitales de Tiempo emitidos por Autoridades de Sellado de Tiempo actuando como agentes completamente externos, independientes e imparciales, en *sensu amplo*, respecto al proceso de notarización.

8. Todos los sellos de tiempo emitidos por una Autoridad de Sellado Temporal o conjunto de ellas, deben estar **irreversiblemente encadenados entre sí**, haciendo que los sellos actuales dependan de muchos, si no de todos, los sellos emitidos con anterioridad.

Todos los sellos de tiempo emitidos por una Autoridad de Sellado Temporal o conjunto de ellas, deben estar irreversiblemente encadenados entre sí, haciendo que los sellos actuales dependan de muchos, si no de todos, los sellos emitidos con anterioridad

Los resultados del encadenamiento de sellos deben difundirse y diseminarse por el mayor número de repositorios públicos posible y con la mayor premura posible; de este modo, ni la propia Autoridad de Sellado Temporal podrá desdecirse de haber generado sus sellos y el público podrá confiar «en lo que ya todos saben o pueden libremente conocer». La publicidad universal de los datos de encadenamiento es lo único que hace realmente irreversible el proceso de sellado, por lo que en ella está la autoridad (moral y) procedimental sobre la que establecer la confianza en el sistema.

9. Al igual que en el caso de la verificación de las pruebas de una transferencia, en la verificación de cualquier Sello Digital de Tiempo tampoco debe participar el agente emisor, sino que debe constituir una actividad independiente y colectiva basada en informaciones públicas y bien diseminadas por la red.

Un sistema, una infraestructura que satisfaga estos principios, muy bien resolvería el problema de la entrega certificada de objetos digitales y, en particular, el de las notificaciones de la Administración a sus administrados como en el caso de las declaraciones del IRPF.

LA 'DIRECCIÓN POSTAL OFICIAL'

Por último, conviene encontrar una solución a lo que ya se planteó en esta sección hace unos meses y que no es cosa distinta del equivalente digital de la «*dirección postal oficial*». El problema es cómo acceder desde la administración a los ciudadanos para hacerles llegar cualesquiera tipos de notificaciones y certificaciones.

Dado que sería ingenuo pensar que todos los ISPs fuesen a dar niveles suficientes de calidad de servicio para las cuentas de correo electrónico de los ciudadanos, y que la fidelidad de sus clientes iba a ser tal que a la administración le permitiese estar segura de que sus envíos a esas direcciones en realidad le llegan al ciudadano y lo hacen a tiempo, la solución de este problema no debería dejarse ni a la iniciativa privada ni a la ciudadanía a título personal.

Una posible solución sería que el Estado Español proporcionara los medios necesarios⁸ para que todos los contribuyentes pudiesen tener cuentas de correo electrónico que actuasen como los «*apartados de correos*» clásicos en los que recibir los mensajes oficiales en general. No se trataría de una cuenta de correo para cualquier uso, ya que sólo aceptaría recibir mensajes «oficiales» adecuadamente firmados, y el ciudadano podría desde ella enviar mensajes a quien quisiera pero con el requisito de que esos envíos fuesen adecuadamente firmados por el titular del «*apartado de correos virtual*». Todo esto ya se puede hacer con software que hay desarrollado en el mundillo universitario español.

La gestión de estos recursos bien podría hacerla un ente proveedor de servicios, estatal o privado, que fuese independiente y estuviese sometido a severas políticas de seguridad que le hicieran desconocer del contenido de los mensajes, y que no pudiese ser parte de ningún proceso entre la Administración y el ciudadano. Esta posible solución es sencilla, y quizá por eso no se ha puesto en marcha todavía ningún piloto que la consagre o la descarte; de todos modos, la realización de soluciones es asunto de la Administración Pública y sus Ministerios, el nuestro es tan sólo hablar, especular y soñar con ello. |

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

7 Un ejemplo de objeto digital protegido podría ser la versión comprimida y cifrada de dicho objeto; cuando se entrega un objeto protegido, todavía falta cierta información para poder disponer libremente de él. Un objeto digital protegido no sirve de nada por sí mismo.

8 Por ejemplo: supongamos 20 millones de contribuyentes, a 100 Mega bytes de espacio de almacenamiento para cada uno de ellos, con lo que tenemos una necesidad de 2 Tera bytes de capacidad. A precios actuales esto supondría unos 16 millones de pesetas. Si queremos hacerlo redundante y tolerante a fallos podríamos estar hablando de 32 millones de pesetas. Aunque la gestión se multiplicase por 10 o por 100 este precio, lo que resulta no es mucho y es una cifra ridícula en los Presupuestos Generales del Estado.