



La Administración Electrónica y sus Sedes

Desde la mañana del 1 de enero de este nuevo año, los ciudadanos españoles tienen derecho a realizar todas sus operaciones administrativas desde Internet. Tal derecho lo reconoce la Ley 11/2007, de 22 de junio, conocida como **Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos**, actualmente en vigor.

Superada la simbólica fecha, la inmensa mayoría de ciudadanos no sabe a qué se parecerá ese paraíso, y eso a pesar de que la Administración dice estar preparada para que el 85% de sus trámites sean telemáticos. Lo que sí es un hecho es que, por el momento, 14 millones de españoles poseen el DNI electrónico, pieza clave de todo el anunciado tinglado, y, con geológica lentitud, algunos de ellos se van dotando de lectores de tarjetas inteligentes para poder conectarlos a su ordenador. La Administración española reconoce que *"la utilización del DNI electrónico no es acorde con el volumen de tarjetas emitidas"*, y el hecho contrastable es que un montón de gente tiene el nuevo documento de identidad y ni lo ha usado, ni sabe cómo hacerlo, ni sabe para qué.

El proyecto de DNI electrónico es un ejemplo de construcción invertida, primero se constituye la infraestructura y luego nos preguntamos para qué sirve. De hecho, a la infraestructura de clave pública del Estado español le queda mucho que explicar al ciudadano para que éste pueda interesarse en amortizar la gran inversión de fondos públicos que ha supuesto y sigue suponiendo esta iniciativa.

Además de la tarjeta física, son necesarios otros elementos

Con la llegada del año 2010, son varias y profundas las transformaciones que el Gobierno español quiere hacer para dar a luz a la, hasta ahora quimérica, Administración electrónica. Hubo una Ley, hay un Real Decreto que la desarrolla un poco, alguna Orden y dos Esquemas Nacionales. Parece que ahora puede ser que realmente se haga algo. En esta entrega pretendemos echar un vistazo razonable a lo que tan ambiciosas iniciativas proponen.

software que deben operar correctamente en los sistemas operativos que van a utilizar el DNle. Dichas piezas software han tardado mucho en salir y no son del todo estables. Los desarrolladores se fijan en sistemas operativos Windows y en Internet Explorer como únicos escenarios, con lo que el resultado cobija incompatibilidades sutiles con otros navegadores como Firefox, o con otros sistemas operativos como Linux.

Dado que la ley de acceso

ciudad española no sepa lo que es realmente una PKI; y eso es primordial para entender qué es y para qué sirve (o podría servir) el DNle.

Iniciativas como www.usatudni.es se quedan tremendamente cortas si tenemos en cuenta la cantidad de recursos invertidos. Las campañas para regalar lectores de tarjetas quizás puedan llegar a calar, pero no resolverán nada, ya que el lector es pieza necesaria, pero no suficiente. El problema de la infraestructura de identidad

electrónica. A través de esas sedes se realizarían *"todas las actuaciones, procedimientos y servicios que requieran la autenticación de la Administración Pública o de los ciudadanos por medios electrónicos"*. Esos sistemas de información deberán *"garantizar la confidencialidad, disponibilidad e integridad de las informaciones que manejan"*, a través de los Esquemas Nacionales de Interoperabilidad y de Seguridad.

En la parte de identificación y autenticación, lo más novedoso del RD es que **habilita la representación de los ciudadanos por terceros**, y crea un registro de representantes y apoderados. En el artículo 16, se propone que, en última instancia, pueda ser el propio funcionario el que identifique y

Ae

Aún queda para que la Administración española y el sector de las TIC conozcan un servicio de entrega/correo electrónico con acuse de recibo que realmente salvaguarde los derechos de los ciudadanos.

no puede discriminar, y no discrimina a los ciudadanos por el sistema operativo que utilicen, ni por el navegador que les resulte más familiar, **es necesario que se alcance la universalidad del middleware relacionado con el DNle**. El sesgo en la elección de los escenarios de prueba y evaluación hace que las aplicaciones que habrían de usar el DNI electrónico en muchos casos fallen, y son esos resultados negativos los que calan en la opinión popular.

Dado que la descripción que se hace de las Infraestructuras de Clave Pública (PKI) en muchos documentos es generalmente embrollada, poco consistente y muchas veces errónea, no es de extrañar que después de tantos años la so-

digital española no está tanto en el hardware como en el software y, sobre todo, en la misma concepción de su uso. Aún así el Ministerio de la Presidencia no pierde su optimismo ni abandona el peligroso voluntarismo filosófico, y está convencido de que resolverán, a corto o medio plazo, unos 545 millones de expedientes anuales, es decir, el 95% de las tramitaciones actuales.

Real Decreto

El Real Decreto 278/2009 de 18 de noviembre de 2009 establece que los órganos de la Administración General del Estado han de crear sus "sedes electrónicas"; es decir sus webs de información y de ventanilla

represente al ciudadano frente al sistema. De este modo, se pretende no dejar a nadie fuera de la Administración electrónica y compensar así el fracaso en el uso del DNle.

En el Capítulo II del texto legal se reconoce la imperiosa necesidad de que esté autenticado lo que aparecerá en esas sedes electrónicas, pero en lugar de aprovechar las circunstancias e inventar lo que sería un **"membrete electrónico"** a incluir en todos los documentos públicos, lo que se hace es dotar a la sede de una identidad digital para el establecimiento de conexiones SSL/TLS. La creación de tal membrete permitiría crear el objeto **"documento público electrónico"**.

Una de las partes más oscu-

ras del RD es la de los "sistemas de Código Seguro de verificación". Esto de los "códigos seguros de identificación" debe ser algo así como firmas digitales simétricas (MAC)¹, ya que tiene que participar la sede electrónica en verificar la integridad. Está claro que hace falta cierta dosis de pedagogía para hacer que estos tipos de documentos inviten al ciudadano a usar el sistema.

Uno de los aspectos peor comprendidos de las tecnologías PKI es el de la verificación de certificados; y el RD opta por crear "Plataformas de Verificación de Certificados" y un "Sistema Nacional de Verificación". Será el Ministerio de la Presidencia el encargado de la gestión de esa plataforma para "la verificación del estado de revocación de [todos] los certificados admitidos en el ámbito de la Administración General del Estado". El servicio se prestará de forma libre y gratuita a todas las Administraciones públicas, españolas y europeas, pero no queda claro si esa verificación también será accesible para todos los ciudadanos.

Una pieza importante del RD es el establecimiento de **Registros Electrónicos** y su obligada existencia y operación en todos los Departamentos Ministeriales de la Administración, para "la recepción y remisión de solicitudes, escritos y comunicaciones". El funcionamiento de estos servicios sería **durante las veinticuatro horas de todos los días del año**, y entregará **recibos digitales**.

Otro nuevo servicio que crea el RD es el de las **comunicaciones y notificaciones electrónicas**. El primero de ellos se centra en poder obligar al ciudadano a comunicar con

la Administración a través de medios electrónicos, lo cual puede simplificar mucho la gestión de algunas convocatorias actuales ya que impediría que el ciudadano pudiera replegarse hacia los procedimientos clásicos en papel.

En cuanto a las **notificaciones electrónicas**, éste es el que más dificultades tiene. Las notificaciones electrónicas podrán efectuarse (1) mediante la **dirección electrónica habilitada**² para ello, (2) mediante **sistemas de correo electrónico**

con acuse de recibo, (3) mediante **comparecencia en sede electrónica**, y (4) mediante otros medios de notificación electrónica "siempre que quede constancia de la recepción por el interesado en el plazo y en las condiciones que se establezcan".

La "Notificación por comparecencia electrónica" lleva al ciberespacio la clásica ventanilla de Correos en la que te entregan un certificado. La ventaja ahora es que la ventanilla estaría en nuestro ordenador al otro lado de un túnel SSL/TLS con autenticación mutua.

Uno de los títulos más

Administración asociará a los documentos una de dos modalidades de referencia temporal: (1) una "Marca de tiempo" como asignación de la fecha y hora; o bien (2) un "Sello de tiempo", que, además de la marca de tiempo, en él intervienen **servicios de certificación externos que aseguran la exactitud e integridad de la misma**. Los sellos de tiempo no tienen equivalente en la administración no-electrónica.

Para atender a las nece-

Ae *Uno de los epígrafes de más claro virtuosismo administrativo y burocrático del RD es el de "los documentos electrónicos y sus copias". Si no fuese porque la copia de objetos digitales conduce a ejemplares indistinguibles entre sí, la presencia de este título hace sospechar que la migración a la dimensión electrónica de la burocracia española se va a hacer "literalmente" sin aprovechar el cambio en la naturaleza del soporte.*

curiosos y de más claro virtuosismo administrativo y burocrático del RD es el de "los documentos electrónicos y sus copias". Después de definir cuáles deben ser las características del documento electrónico, se define lo que se entiende por metadatos, cómo se añaden al documento y cómo le aportan cualidades al mismo: en particular, la de "ser copia de". Con todo ya preparado, el RD actualiza el concepto de "compulsión electrónica". Si no fuese porque la copia de objetos digitales conduce a ejemplares indistinguibles entre sí y, por tanto, no se puede saber quién es copia y quién original, la presencia de este título hace sospechar que la migración a la dimensión electrónica de la burocracia española se va a hacer "literalmente" sin aprovechar el cambio en la naturaleza del soporte.

Algo muy importante en la versión electrónica es la "Referencia temporal de los documentos administrativos electrónicos", por la que la

sidades de almacenamiento y conservación, el RD precisa la creación de **Archivos Electrónicos de Documentos**, aunque no se dan muchas pistas sobre cómo hacerlo. Sin embargo, se deja abierta la posibilidad, bastante avanzada, de "conservación de documentos electrónicos mediante la inclusión de su información en bases de datos", pero con la precaución de que se guarde la información necesaria para reconstruir los documentos originales y se pueda verificar toda firma electrónica que hubiera sobre ellos.

Resuelto el problema del archivar, es fácil transportar al mundo telemático el concepto de "expediente electrónico", y eso es a lo que se consagra el séptimo capítulo del Real Decreto.

Para poder imaginar una administración electrónica hay que poner orden en las informaciones, formatos, objetos, transacciones, procedimientos, etc., que se vayan a utilizar. Además, también hay que clasificar la información según

¹ MAC = Message Authentication Code; normalmente se construyen sobre funciones *hash* haciéndolas controlables por una clave simétrica secreta.

² Ver <http://www.correos.es/contenido/05P-Otros/09-DireccionElectronica/05P09-DireccionElectronica.asp>

su nivel de riesgo; sin ello, es del todo imposible aportar seguridad al sistema.

Esquemas Nacionales

En el Artículo 42 de la ley 11/2007, se crea el **Esquema Nacional de Interoperabilidad**³ (ENI) como el "conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas". El objetivo básico es garantizar la interoperabilidad técnica, semántica y organizativa dentro de la Administración electrónica española, lo cual no es baladí.

En materia de seguridad, el ENI remite directamente al Esquema Nacional de Seguridad (ENS) con el que pretende ser complemento perfecto para dar cuerpo a la futura administración electrónica.

En el artículo 42.2 de la Ley 11/2007 se crea el **Esquema Nacional de Seguridad (ENS)**⁴ para fijar los principios y requisitos mínimos de la política de seguridad, con el fin de utilizar medios electrónicos y proteger la información que fluye y se almacena en ellos. El ENS establece las condiciones necesarias (¿y suficientes?) que den confianza en los sistemas buscando la seguridad de los mismos, los datos, las comunicaciones y los servicios electrónicos.

La "seguridad" se entiende como "la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes, acciones ilícitas o malintencionadas, que comprometan la disponibilidad, autenticidad,

integridad, confidencialidad y trazabilidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen, o a través de los que se realiza el acceso".

El ENS también determina los tipos de información, las dimensiones de la seguridad y cuáles son sus niveles, cuáles las categorías de los sistemas, las medidas de seguridad adecuadas en cada caso y la necesaria auditoría periódica de la seguridad. En esta norma se exige también la elaboración

de algo sin haberlo evaluado previamente, de forma imparcial y a fondo, muy a fondo.

Supongo que escarmenando en cabeza ajena, el ENS presta "especial atención a la información almacenada o en tránsito a través de entornos inseguros" (portátiles, PDAs, smartphones, periféricos, pendrives, comunicaciones sobre redes abiertas o con cifrado débil, GSM, etc.). Sin embargo, esto no pasa de ser una declaración de intenciones sobre un tema que tiene

quizás algo de seguridad, en los procesos e instrumentos que utilizan las administraciones de este país.

El objetivo de estas piezas legales es muy ambicioso y no se le debe restar apoyo, dado que es el futuro lo que se juega la Administración española, si no logramos modernizar, hacer más eficaces, más seguras y más cómodas las relaciones administrativas. La burocracia es algo tremendamente arraigado en nuestra sociedad y, en algunos casos, puede servir de garante de los

Ae *Para poder hacer segura la futura Administración electrónica es absolutamente necesario simplificarla. El oscurantismo decimonónico que todavía hoy persiste tan sólo sirve para hacer convenientemente insegura e ineficaz la actual Administración española.*

regular de un informe sobre la seguridad real de los sistemas de información y se explicita el papel del CCN-CERT⁵ en la respuesta ante incidentes de seguridad que se puedan producir.

El ENS indica que la Administración se va a tomar en serio el control de lo que ocurre en sus sistemas de información de modo que las actuaciones de todos los agentes "serán supervisadas para verificar que se siguen los procedimientos establecidos". Si esto es así, está claro que no podrá hacerse nada en la administración pública que sea anónimo; lo cual está muy bien.

Muestra clara del posibilismo que hay en el ENS es que, cuando habla de las adquisiciones de materiales y productos de seguridad TIC, indica que "se valorará positivamente la certificación de las funcionalidades de seguridad", pero no se exige, lo cual puede hacer pensar (erróneamente) que se puede confiar en la se-

más complicaciones de las que aparenta.

Entrando ya en cuestiones más técnicas, en el texto se define lo que es **Información Administrativa**, y una vez identificada la sustancia de la actividad administrativa, el ENS define tres niveles de seguridad: **Alto, Medio y No-divulgable**, según el efecto que tenga su revelación para el procedimiento o los intereses de las personas afectadas.

En los anexos técnicos es donde se define como **dimensiones de la seguridad: Disponibilidad, Autenticidad, Integridad, Confidencialidad y Trazabilidad**, y a cada una de ellas se la puede calificar como de nivel **BAJO, MEDIO o ALTO**, o no se le asignará nivel si no se ve afectada.

Podríamos seguir desmenuzando detalles técnicos del ENS pero lo interesante es resaltar que con él se convierte en Real Decreto un manual básico para el diseño de políticas de seguridad. Dado que en la Administración esto no se había hecho todavía, la aparición del ENS podría ser un avance significativo a la hora de poner orden, y

derechos de los ciudadanos, pero muchas otras de las veces sólo supone un grave lastre para el funcionamiento de nuestra sociedad.

El paso a la Administración electrónica no debería hacerse como mera transustanciación de lo que ya llevamos centenares de años haciendo, sino que debemos aprovechar el cambio tecnológico para forzar una metamorfosis que la haga mejor, más eficaz y más justa. No es sólo un problema de hardware o software variados, es un problema de planteamiento. Para poder hacer segura la futura Administración electrónica es absolutamente necesario simplificarla. El oscurantismo decimonónico que todavía hoy persiste tan sólo sirve para hacer convenientemente insegura e ineficaz la actual Administración española. ■

JORGE DÁVILA MURO
Consultor independiente
Director
Laboratorio de Criptografía
**LSIIS – Facultad
de Informática – UPM**
jdavila@fi.upm.es

³ Ver <http://www.csa.e.map.es/csi/pg5e41.htm>

⁴ Ver <http://www.csa.e.map.es/csi/pg5e42.htm>

⁵ Ver <https://www.ccn-cert.cni.es/>