Tendencias pan-europeas en gestión de identidad digital

POR **SERGIO SÁNCHEZ**

En el año 2006, la Unión Europea lanzó su *i2010 e-Government Action Plan* (Comisión Europea, 2006), destinado a modernizar y hacer más eficaces los servicios públicos de los Estados Miembros, recogiendo el derecho de los ciudadanos a un acceso seguro y cómodo a los servicios y estableciendo sistemas para el reconocimiento mutuo de las identidades electrónicas en los servicios de la Administración Pública, tratando de reducir la carga de burocracia e ineficacia a la que actualmente se enfrentan los ciudadanos. En este concepto de modernización y mejora se contempla como un requisito fundamental la continuidad transfronteriza de los servicios públicos, de manera que sea posible la realización de trámites donde estén involucradas las Administraciones Públicas de distintos Estados.

Cómo afrontar la identidad digital

A lo largo de los últimos años y quizás de forma más contundente en la actualidad, podemos afirmar que nos encontramos en un entorno cada vez más digital en el que el uso de las nuevas tecnologías y la presencia, tanto de las personas como de las entidades, en Internet ha propiciado un nuevo escenario de interacción, cada vez más global y distribuido. En este entorno digital y global, quizás una de las carencias más significativas sea la de una gestión fiable de la identidad digital que permita una traslación con garantías de lo que podríamos llamar procesos o transacciones tradicionales basados en la identidad al ámbito de la Red. Una de las demandas tradicionales de los ciudadanos es la de disponer de una identidad «única» e integrada en la Red, es decir, disponer de una única credencial que les permita acceder a todos los servicios ofrecidos por un determinado proveedor de servicios, independientemente de que este sea de tipo gubernamental o no y los servicios sean de carácter público o privado. Con la globalización surgen nuevos retos desde el punto de vista de la identidad y su gestión y, asociados a ellos, nuevos problemas a solventar. En este sentido existen distintos enfoques, tendencias o futuros escenarios de cara a hacer frente al problema que podríamos denominar de la gestión de la identidad, tal como se recoge en (Schwartz, 2011).

El primero de ellos sería el de continuar con el sistema ya implantado en la Red, que podríamos denominar «del sector privado», en el que existen proveedores de identidad que nos autentican y controlan los datos de identidad que les proporcionamos, normalmente de forma voluntaria, que pueden o no proteger nuestra privacidad y que se pueden basar en

soluciones abiertas o totalmente propietarias. El segundo sería el basado en el sector privado, pero con cierto grado de supervisión. Es el caso, por ejemplo, de la NSTIC (*National Strategy for Trusted Identities in Cyberspace*), una iniciativa del gobierno de los Estados Unidos en la que se trata de hacer frente al problema de la gestión de identidad y la privacidad tomando el liderazgo del sector privado y combinando sus iniciativas con aquellas derivadas de la protección del consumidor.

Por último, el tercero, sería aquel en el que el gobierno o los gobiernos de un grupo de países trabajan de forma conjunta para proporcionar las soluciones demandadas al problema de la gestión de identidad, creando un sistema de gestión de identidad gubernamental que permita el acceso a los servicios proporcionados por las administraciones, pero que a su vez pueda ser utilizado por el sector privado. Es este último camino el que se ha adoptado en la Unión Europea (UE).

En este mismo sentido, y continuando con la línea establecida por el Plan i2010, a finales de 2010 se publicó el *eGovernement Action Plan 2011-2015* (Comisión Europea, 2010), que fija entre sus prioridades el establecimiento de sistemas interoperables tanto en el ámbito de la identificación como en el de la autenticación en la UE.

Como consecuencia inmediata de la aplicación del Plan i2010 nos encontramos con que las Administraciones Públicas (a nivel nacional, regional y local) de todos los Estados miembros deben atender las actuaciones administrativas de los ciudadanos a través de Internet. Ello conlleva la puesta en marcha de una serie de medidas adicionales, tanto a nivel nacional como internacional, destacando por su impacto directo en los ciudadanos la necesidad de que estos dispongan de una identificación digital que les permita autenticarse inequívocamente al realizar las gestiones a través de Internet.

Se puede decir que una identidad digital es la representación electrónica de un determinado conjunto de atributos de identidad que no tienen que ser necesariamente únicos pero que son útiles en la medida en que, de forma conjunta, permiten distinguir a una entidad de otra. Conforme a esta definición, para una entidad dada, típicamente existirán múltiples identidades digitales que pueden ser únicas o no.

Tanto en los países que ya disponen de sistemas de identificación tradicionales como en los que no los tienen, será preciso dotar a los ciudadanos de dicha identidad digital, de manera que les permita identificarse en la Red, al menos, con las mismas garantías con las que lo hacen con su sistema de identificación tradicional en las interacciones interpersonales. En este sentido, en la mayoría de los países pertenecientes a la UE se está desplegando la infraestructura que permita, en un plazo razonable de tiempo, la expedición a todos sus ciudadanos de tarjetas de identificación electrónicas, denominadas *eID cards*, cuyo aspecto exterior es similar al de los documentos de identificación tradicional, pero con la salvedad de que incluyen un chip donde se almacena la información sobre la identidad del ciudadano. Estas *eID cards* están ya siendo expedidas en Austria, Bélgica, Estonia, Finlandia, Italia, Portugal, Suecia y España.

En el Plan i2010 no se contemplaba que las tarjetas de identificación tradicionales debieran

evolucionar hacia las *eID cards*, ya que las primeras fueron concebidas para su utilización en servicios públicos relacionados con la seguridad del Estado, como por ejemplo para facilitar el control en las fronteras, mientras que la identificación electrónica busca facilitar tanto el acceso a servicios públicos como la oferta de servicios personalizados. Sin embargo, países como España, han optado por recoger la funcionalidad de ambos tipos de tarjeta en un único elemento, en la línea de lo sugerido por los estándares para la tarjeta de ciudadano europeo, concretamente la parte 4: *Identification card system – European Citizen Card – Part 4: Recommendations for European Citizen Card issuance, operation and use* (CEN, 2012).

No obstante, a pesar de las ventajas que indudablemente conlleva para los ciudadanos de la UE el hecho de poseer una identidad digital que les permita el acceso seguro e identificado a los servicios ofrecidos por las distintas Administraciones Públicas, la puesta en marcha de esta solución no está exenta de riesgos que, si no son debidamente abordados, pueden mermar la eficacia y confianza de los ciudadanos en las instituciones del Estado.

Problemas asociados a la identidad digital en el marco de la UE

Cabe destacar que no se abordan aquí los riesgos inherentes a cualquier proceso de registro y autenticación derivados del hecho de que elementos maliciosos se apropien indebidamente de las credenciales de un ciudadano (y, a partir de ahí obtengan su identidad electrónica) o se adueñen de la propia identidad electrónica. Cualquiera de estas circunstancias podría ocasionar importantes daños, entre los que cabe destacar la pérdida de integridad y confidencialidad de la información y la pérdida de disponibilidad y funcionalidad de un servicio, pudiendo conllevar riesgos de pérdida financiera para las instituciones y los ciudadanos e incluso riesgos para la seguridad personal de estos últimos.

Debido a la gran trascendencia de este problema, desde hace años se han invertido importantes esfuerzos en conseguir que el proceso de registro de los ciudadanos ante las Autoridades de Registro a la hora de emitir elementos de identidad digital cuente con las máximas garantías de seguridad, forzando a estas Autoridades a que verifiquen exhaustivamente las credenciales presentadas y obligándolas a mantener fuertes medidas internas de seguridad[1]. En este sentido, quizás el aspecto que debe ser reforzado es el que concierne al ciudadano, ya que debe concienciarse de los riesgos que conllevan la posesión de una identidad digital y la necesidad de protegerla en todo momento.

Interoperabilidad entre sistemas de gestión de identidad de la UE

Un importante reto que deben afrontar los sistemas de identificación digital es la continuidad transfronteriza de los servicios públicos, esto es, que un ciudadano no encuentre barreras difíciles de franquear, o incluso imposibles, para acceder a servicios públicos ofrecidos por distintos países. A día de hoy un ciudadano español puede trabajar para una empresa alemana y desarrollar su labor profesional en Bélgica sin, teóricamente, ningún tipo de traba administrativa. Sin embargo, en este entorno multinacional, cuando el trabajador desea acceder con su tarjeta de identidad nacional emitida en España, a los servicios ofrecidos por la Administración Pública alemana o consultar los datos de su vida laboral en la Administración Pública belga, surgen problemas derivados de la necesidad de validar la identidad digital del

ciudadano a través de un certificado digital emitido por una entidad de un país distinto a aquel desde el que se está solicitando el servicio.

Uno de los problemas fundamentales en el uso de la identidad digital es el de la interoperabilidad a nivel pan-europeo desde el punto de vista de los sistemas de gestión e identidad. De forma genérica, dada la diversidad de sistemas de gestión, cuando el usuario de un sistema dado, ya sea un ciudadano, una empresa o la propia Administración, quiere comunicarse con administraciones fuera del ámbito de su sistema de gestión de identidad, debe existir una relación entre los sistemas de gestión involucrados, de tal forma que la identidad de los usuarios de uno sea entendida y aceptada por el otro. Se hace necesario, por lo tanto, el establecimiento de un marco de interoperabilidad entre sistemas de gestión de identidad a nivel de la UE que incluya la especificación y el desarrollo de un conjunto de infraestructuras técnicas y organizativas que permitan definir, administrar y gestionar los atributos de identidad de los ciudadanos y entidades. Para ello, la Unión Europea fijó un mapa de ruta (Comisión Europea, 2007) en el que se establecen una serie de principios de diseño en torno al principio fundamental de la subsidiaridad, es decir, cada Estado miembro debe mantener su autonomía y responsabilidad para continuar con sus iniciativas de Sistemas de Gestión de Identidad.

Uno de los conceptos básicos establecidos en el mapa de ruta es el de la federación de identidad, es decir, debe existir una confianza mutua entre las distintas Administraciones en lo que se refiere a los métodos de identificación y autenticación. Esto es, la federación de identidad hace referencia a un esfuerzo común por conseguir la interoperabilidad de los Sistemas de Gestión de Identidad presentes en distintos entornos. De esta manera la información sobre la identidad de un usuario, posiblemente distribuida entre distintos entornos, puede aglutinarse para que este se pueda autenticar en un entorno y acceder a los demás. Asimismo, los distintos proveedores de servicios pueden acceder a los datos de usuario presentes en los distintos entornos.

La federación de identidad extiende el uso de la identidad digital de un usuario, de forma que pasa de ser algo interno a un proveedor de servicios a ser común a varios de estos proveedores. Este cambio propicia la aparición de complicados procesos de gestión relativos a la forma en la que la identidad es registrada, revocada y modificada dentro de un proveedor de identidad, de manera que la federación de identidad está sujeta, obviamente, a mayores riegos de seguridad.

Tomando como base lo establecido en los planes de acción y lo comentado anteriormente, a lo largo de los últimos años han surgido en el ámbito de la UE distintas iniciativas (Modinis, 2005; Bruegger, Hühnlein y Schwenk, 2007; Guide, 2004, y Stork, 2008) enfocadas a la consecución de la interoperabilidad pan-europea de los sistemas de gestión de identidad. Básicamente en todas ellas se propone la creación de una infraestructura de seguridad basada en un modelo federado que confía en una serie de portales de identidad en cada Estado miembro responsables de la autenticación de las entidades a nivel nacional y de establecer criterios de aceptación y niveles equivalentes de confianza para las autenticaciones realizadas en otros Estados.

Confianza, interoperabiidad a nivel semántico y protección de datos personales

Quizás uno de los problemas más importantes en este caso sea el de la confianza. La heterogeneidad de los sistemas existentes y de los mecanismos de autenticación y autorización utilizados en los distintos países hace que el equipar al sistema pan-europeo con la capacidad de mapear los niveles de confianza otorgados a los distintos mecanismos de autenticación en los distintos países sea crucial si se pretende conseguir que el acceso a los servicios sea lo más transparente posible a los usuarios.

Otro importante problema a solucionar es el de la interoperabilidad desde el punto de vista semántico. El hecho de incorporar a un sistema global, en este caso pan-europeo, soluciones ya implementadas a nivel nacional, hace que sea necesario establecer mecanismos de traducción en lo referente a los formatos de representación de la información, convirtiendo en imprescindible el alcanzar cierto grado de interoperabilidad desde el punto de vista semántico.

A pesar de la existencia de los planes de acción y del mapa de ruta que establece, entre otras cosas, unos principios de diseño, se puede afirmar que, en la práctica, la interoperabilidad entre los sistemas de gestión de identidad de distintos países en Europa sigue siendo más una ambición que una realidad, aunque se están proponiendo soluciones.

Un último aspecto a destacar es el de la protección de los datos de carácter personal. En la actualidad, la identidad de una persona física no está sistemáticamente regulada por la legislación. Existe un conjunto de definiciones que no siempre coinciden entre sí y que tienen fundamentalmente dos funciones: permitir la identificación con fines legales y proteger los derechos individuales y libertades relacionados con una persona física. En lo que se refiere a la regulación, se puede decir que la identidad personal está regulada en los distintos niveles, puesto que se aborda en las constituciones nacionales, en el tratado de la Unión Europea, en las legislaciones privadas de cada nación, en la legislación administrativa y está protegida además frente a accesos y usos no autorizados por parte de terceros mediante la ley criminal.

De forma genérica podemos decir que un método de identificación que permita diferenciar a un individuo de todos los demás debe cumplir, desde el punto de vista legal, dos reglas fundamentales: mostrar suficiente información para garantizar el mayor grado de seguridad posible a la hora de diferenciar a un individuo de los demás y no mostrar información que corresponda al plano privado del individuo a identificar.

Normalmente, y para cumplir con lo anterior, cada sistema legal dispone en sus documentos de identificación de un conjunto de información que suele corresponder con una imagen biométrica de una o más partes del cuerpo del sujeto a identificar, como es el caso del DNI español. De cualquier forma, en algunos países como Austria o Reino Unido no es obligatorio portar ningún documento de identificación, a diferencia de lo que ocurre en otros países como España, Italia o Alemania, donde sí lo es.

Directiva europea 95/46/CE sobre protección de datos

Con la intención de reforzar la confianza de los ciudadanos en los sistemas de identificación

electrónica y de unificar la legislación, se estableció la Directiva Europea 95/46/CE sobre protección de datos (Parlamento Europeo, 1995), cuya finalidad es otorgar al sujeto el mayor control posible sobre su identidad y datos personales, planteando una serie de requisitos a cumplir por los receptores, controladores, procesadores y terceras partes a la hora de manejarlos. En este contexto se entiende como datos personales «toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social».

Así, cabe destacar de entre los principios que establece dicha Directiva los siguientes:

- Los datos personales deben ser procesados adecuadamente y cumpliendo completamente con lo establecido en la ley, deben ser recogidos con unos propósitos explícitos y legítimos, ser relevantes y adecuados a dichos propósitos (nunca excesivos) y ser utilizados de acuerdo a los mismos. Este principio se extiende a la cooperación entre administraciones, necesaria para recabar datos específicos de un ciudadano concreto, lo que conllevará que una administración solicite a otra esos datos en nombre o representación de ese ciudadano.
- Los datos que permitan identificar a un individuo no deben ser retenidos más tiempo del necesario y es preciso proporcionar a los individuos medidas de control para rectificar, borrar o bloquear los accesos a sus datos personales, adoptándose además las medidas apropiadas, tanto desde el punto de vista técnico como organizativo, para evitar el acceso no autorizado o el uso ilegítimo de los datos.
- Los datos personales no deben ser transferidos a un país o territorio fuera del Área Económica Europea a no ser que el país o territorio asegure un nivel de protección adecuado sobre los mismos.

A pesar de la existencia de estos principios aplicables a los datos personales, existen muchos recelos respecto a la posibilidad de que en las tarjetas de identificación electrónica se incluya información adicional sobre su poseedor que permita un mayor control por parte del Estado del ciudadano (por ejemplo, que incluya información sobre su ideología política, creencias religiosas, enfermedades socialmente rechazadas, o que permita rastrear sus movimientos).

Este miedo es aún mayor cuando, como en el caso de España, se recogen en un único documento los datos requeridos para la autenticación tanto en servicios relacionados con la seguridad del Estado como en aquellos relacionados con la interacción entre el ciudadano y la Administración Pública. Por tanto, uno de los retos a los que se enfrentan los sistemas de identificación digital es el de dotarles de la máxima transparencia, para que los ciudadanos no alberguen ninguna sospecha sobre la naturaleza de los datos personales que porta la tarjeta que poseen.

Conclusiones

Cada vez son más habituales los desplazamientos de los ciudadanos de los países miembros dentro de la Unión Europea por razones de trabajo o estudio y todo parece indicar que esta

tendencia se acrecentará a medida que la cooperación entre países dentro de la UE sea más intensa y el número de proyectos e iniciativas de titularidad pan-europea se incremente.
Por otra parte, es previsible que aumente el número de personas que se desplacen dentro de Europa durante periodos largos de tiempo por deseos personales, por ejemplo, el caso de personas jubiladas que cambien su lugar de residencia porque prefieran vivir en zonas apacibles, pero que quieran mantener su nacionalidad de origen.

La distribución paulatina, pero decidida, de tarjetas inteligentes con funciones de eID card proporciona elementos indispensables para la implementación de los sistemas de gestión de identidad. No obstante, a pesar de las indudables ventajas que conlleva para los ciudadanos de la UE el hecho de poseer una identidad digital que les permita el acceso seguro e identificado a los servicios ofrecidos por las distintas Administraciones Públicas de los Estados miembros, la puesta en marcha de una solución de este tipo conlleva una serie de riesgos que, si no son debidamente tratados, pueden llegar a traducirse en una merma en la eficacia y confianza de los ciudadanos en las instituciones públicas.

Aunque los sistemas de gestión de identidad de ámbito pan-europeo son tecnológicamente factibles, se debe tener en consideración que la interoperabilidad en materia de gestión de identidad no es solo un problema tecnológico, sino que existen importantes barreras legales que afectan a las relaciones transfronterizas y transectoriales y para las cuales la UE debe proporcionar el soporte legal adecuado antes de lograr la interoperabilidad deseada.

Es opinión del autor que, a pesar de los inconvenientes enumerados, en la medida en que se solucionen los problemas mencionados y los sistemas de identificación digital vayan ganando la confianza de la población, se logrará la interoperabilidad en materia de gestión de identidad.

Referencias

Bibliografía

Bruegger, B. P., Hühnlein, D. y Schwenk, J. (2007). *TLS-Federation – a Secure and Relying-Party-Friendly Approach for Federated Identity Management* [en línea]. Disponible en: *http://porvoo14.dvla.gov.uk/documents/tls_federation_final.pdf*

Comisión Europea (2006). *I2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All* [en línea]. Bruselas. Disponible en: *http://ec.europa.eu/information_society/activities/egovernment/docs/action_plan/comm_pdf_com_2006_0173_f_en_acte.pdf*

Comisión Europea (2007). *A Roadmap for a pan-European eIDM Framework by 2010*. Version 1.0. [En línea] Disponible en: *http://ec.europa.eu/information_society/activities/egovernment/docs/pdf/eidm_roadmap_paper.pdf*

– (2010, 15 de diciembre). *The European eGovernment Action Plan 2011-2015. Harnessing ICT*

to promote smart, sustainable & innovative Government. COM(2010) 743.

Comité Europeo de Estandarización (CEN) (2012). *Identification card system – European Citizen Card – Part 4: Recommendations for European Citizen Card issuance, operation and use*. CEN/TS 15480-4.

Graux, H. y Majava, J.(2007, diciembre). *eID Interoperability for PEGS: Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms* [en línea]. Disponible en: *http://ec.europa.eu/idabc/servlets/Doc?id=29622*

GUIDE (2004). *Creating a European Identity Management Architecture for eGovernment* [en línea]. Disponible en: *http://istrg.som.surrey.ac.uk/projects/guide/overview.html*

ModinisIDM (2005)
https://www.cosic.esat.kuleuven.be/modinisidm/twiki/bin/view.cgi/Main/WebHome

Parlamento Europeo; Consejo de la Unión Europea (1995). *Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. Diario Oficial de la Comunidad Europea. Luxemburgo, 23 de Noviembre de 1995. Vol. L, 281, 31-50.

Schwartz, A. (2011, junio). Identity Management and Privacy: A Rare Opportunity To Get It Right. *Communications of the ACM,* 54(6), 22-24.

Stork (2008). *Secure idenTity acrOss boRders linked* [en línea]. Disponible en: *http://www.eid-stork.eu/*

VVAA. *eGovernment: Commission calls for ambitious objectives in the EU for 2010* [en línea]. Disponible en:
http://europa.eu/rapid/pressReleasesAction.doreference=IP/06/523&format=PDF&aged=1&language=EN&guiLanguage=en

Notas

1 Un estudio detallado de los riegos que existen en los procesos de registro y autenticación, sus posibles impactos en instituciones y ciudadanos y las probabilidades de ocurrencia puede encontrarse en Graux y Majava (2007).