Gestión de Identidad en las Administraciones Públicas: Interoperabilidad pan-Europea

Sergio Sánchez García, Ana Gómez Oliva,

DIATEL – EUITT – Universidad Politécnica de Madrid, Ctra. Valencia Km.7, 28031 Madrid, Spain
sergio@diatel.upm.es, agomez@diatel.upm.es

Resumen. En un entorno digital y cada vez más global, la provisión de servicios basados en la identidad electrónica de una persona o entidad y la gestión de dicha identidad por parte de las Administraciones Públicas constituyen un importante reto, muy especialmente cuando los ciudadanos, y en general las entidades a autenticar, presentan acreditaciones procedentes de distintos países y, por tanto, ajustadas a la legislación particular de cada uno de ellos. En este artículo se recogen y analizan las soluciones propuestas hasta la fecha en el marco de la Unión Europea y se presenta la propuesta de una infraestructura totalmente interoperable para gestión de identidad que está desarrollando este grupo de investigación. La novedad de esta propuesta reside en que puede emplearse tanto para la interoperabilidad con otros países europeos como entre los distintos niveles de la Administración española (local, autonómico y central).

Palabras clave: eID, eIDM, identidad electrónica, sistemas de gestión de identidad electrónica, pan-Europeo.

1 Introducción

En algunos países europeos existe tradicionalmente un sistema de identificación de ciudadanos basado en un documento que éstos poseen y que les identifica de forma unívoca. A pesar de los distintos nombres que recibe en función del país (Documento Nacional de Identidad en España, Tarjeta de Ciudadano en Bélgica, etc.) su contenido y funcionalidad son prácticamente similares en todos ellos. Normalmente este documento ha ido evolucionando a lo largo del tiempo, pasando por distintos formatos, desde una simple hoja de papel que contenía un conjunto de datos personales "certificados" por una autoridad oficial a los más recientes documentos de identidad con fuertes medidas antifalsificación y datos adicionales, como por ejemplo fotografía y huella dactilar, que permiten una identificación biométrica y, presumiblemente, más fiable de su poseedor. A pesar de la evolución en el formato, la funcionalidad y ámbito de aplicación de los documentos de identificación se puede considerar estancada. Este tipo de tarjetas ha servido tradicionalmente como medio de identificación del ciudadano ante la Administración Pública de su país y,

adicionalmente, es utilizado por las empresas privadas como medio de identificación de los usuarios de sus servicios, puesto que su identidad está reflejada en el mismo y los empleados pueden verificarla visualmente de forma directa. Sin embargo, la aparición de Internet y el paulatino acercamiento de los ciudadanos a la sociedad digital han provocado un cambio en este aspecto. Cada vez más trámites, tanto con la Administración como con los proveedores de servicios, se realizan a través de la Red y, por lo tanto, existe una creciente demanda de sistemas de identificación que permitan realizar este tipo de transacciones sin pérdida de garantías en cuanto a la seguridad. Por tanto, es preciso dotar a los ciudadanos de una *identidad electrónica* o *digital* que les permita identificarse en la Red, al menos, con las mismas garantías con las que lo hace con su tarjeta de ciudadano en las interacciones interpersonales.

Con la intención de subsanar el problema anterior, en la mayoría de los países pertenecientes a la Unión Europea se está llevando a cabo la implantación de tarjetas de identificación electrónicas, también denominadas *eID cards*, cuyo aspecto exterior es similar al de los documentos de identificación actuales pero con la salvedad de que se incluye un chip que permite el almacenamiento electrónico de información sobre la identidad, así como la interacción con ciertas aplicaciones, de forma que el usuario pueda demostrar digitalmente su identidad.

Además de un entorno cada vez más digital, los ciudadanos europeos, al igual que los del resto del mundo, se encuentran en un entorno cada vez más global. 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 y, adicionalmente, debe poder llevar a cabo interacciones a través de la Red tanto con su empresa como con las Administraciones Públicas de los distintos países. Este entorno global da lugar a una serie de problemas que surgen cuando nos planteamos, por ejemplo, cuestiones del siguiente tipo: ¿cómo el ciudadano, con su tarjeta de identificación electrónica de España accede a los servicios ofrecidos en la Red por la Administración Pública alemana?, ¿y a sus datos como trabajador en Bélgica?, es más, ¿cómo gestiona la Administración Pública alemana los datos de identidad del ciudadano? La respuesta a estas preguntas no es sencilla, pero en todo caso pasa por la especificación y el desarrollo de un conjunto de infraestructuras técnicas y organizativas que permitan la definición, administración y gestión de los atributos relativos a la identidad de los ciudadanos. Estas infraestructuras reciben el nombre de Sistemas de Gestión de Identidad (*Identity Management Systems* o *IDMs*).

Este artículo recoge, en primer lugar, una visión general del estado actual de los sistemas de gestión de identidad a nivel pan-Europeo, analizando las principales propuestas realizadas hasta la fecha en el marco de la Unión Europea e identificando aquellos puntos sobre los que ya existen unos principios de acuerdo y aquellos otros pendientes de solución que impiden hasta la fecha la adopción de un modelo a gran escala. A continuación se presenta la propuesta de arquitectura de interoperabilidad sobre la que está trabajando este grupo, que da solución a los problemas detectados y que presenta como particularidad que no sólo puede emplearse para la interoperabilidad de los sistemas de gestión entre distintos países europeos, sino que la solución es extrapolable a las distintas esferas de la Administración Pública española (local, autonómica y central). Por último, se comenta la experiencia piloto que se está realizando para poner en marcha las soluciones adoptadas.

Esta propuesta se enmarca dentro de los trabajos que este grupo de investigación lleva a cabo en el proyecto TSI2006-4864 *Plataforma telemática de Administración Electrónica basada en coreografía de servicios* subvencionado por el Ministerio de Educación y Ciencia, en el Plan nacional de I+D+I.

2 La Identidad y la Identidad Digital

Antes de comenzar a hablar de sistemas de gestión de identidad conviene dejar claro lo que se entiende por identidad y por identidad digital.

De acuerdo a [1] el concepto de identidad se puede definir desde tres puntos de vista distintos, el sociológico, el legal y el tecnológico. El punto de vista sociológico, que evidentemente debe ser estudiado y considerado por expertos en la materia, queda fuera del ámbito del estudio que se pretende realizar en este artículo, por lo que nos centraremos en la parte legal y tecnológica. Partiendo de esta consideración nos encontramos con que la identidad del individuo está compuesta, por un lado, por elementos encargados de garantizar la unicidad de una persona física y, por otro, por elementos que son la expresión de la identidad humana en todos sus posibles aspectos. Desde el punto de vista legal podemos decir que la **identidad personal** está formada, tradicionalmente, por el conjunto de datos resultantes de la unión de la información relativa a una persona presente en los registros públicos que va a permitir identificarla de forma unívoca. Podemos afirmar que a mayor cantidad de información sobre una persona, más "única" es esa persona. Por otra parte, ese tipo de información como puede ser el estado civil o la profesión, son consideras por la legislación actual como superfluas a la hora de la identificación personal por estar demasiado ligadas a la esfera privada del individuo. La Directiva Europea 95/46/CE sobre protección de datos [2] tiene como finalidad el 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. El artículo 2, letra a) define *datos personales* de la siguiente forma:

> *"«datos personales»: toda información sobre una persona física identificada o identificable (el «interesado»); 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"*

El concepto de **Identidad Digital** o Identidad de Red como la denomina la Liberty Alliance [3] surge como consecuencia de la interacción de los usuarios con los servicios que les son ofrecidos a través de la Red. Cuando los usuarios interactúan con los servicios a menudo los personalizan de acuerdo a sus preferencias o necesidades, de manera que además de establecer unos datos de acceso como nombre de usuario y contraseña establecen otros parámetros como, por ejemplo, la información que desean que se les muestre, la disposición de los elementos en la página que ofrece el servicio

o la forma de notificar los cambios en el mismo. Normalmente el establecimiento de una cuenta y la personalización de la misma se realiza por parte de los usuarios para cada uno de los proveedores de servicio a los que accede, de forma que el usuario dispone de múltiples cuentas con múltiples parámetros. De acuerdo a la Liberty Alliance la Identidad de Red de un usuario está constituida por el total de los conjuntos de atributos que constituyen las distintas cuentas de un usuario.

Concretamente en el draft *Liberty ID-FF Architecture Overview* [4] se define la Identidad de Red con la siguiente frase:

> *"A network identity is the global set of attributes composed from a user's account(s)."*

Para una entidad dada, típicamente existirán múltiples identidades digitales que pueden ser únicas o no. Una identidad digital es, por definición, un subconjunto de la identidad y puede ser considerada como la manifestación de la entidad en la Red.

3 Sistemas de Gestión de Identidad y Globalización

De acuerdo a la definición dada en [5], se considera un Sistema de Gestión de Identidad como la infraestructura técnica y organizativa para la definición, gestión y administración de atributos de identidad.

A lo largo de los últimos años en todos los estados miembros de la Unión Europea se están desarrollando iniciativas para la introducción de identidades electrónicas (eID) en los servicios públicos y los correspondientes sistemas de gestión de dichas identidades. La utilización de este tipo de sistemas de gestión y de las identidades electrónicas resulta muy útil a los ciudadanos en cuanto que les permite un acceso mucho más rápido y eficaz a los servicios ofrecidos por las Administraciones Públicas pero, tal como se comentó en la introducción, surgen problemas debido a la globalización. La identidad electrónica de un ciudadano le permite operar correctamente dentro del entorno correspondiente a su propio país pero ¿qué ocurre cuando ese entorno pasa a ser el formado por el conjunto de países de la Unión Europea? El documento de identidad de un ciudadano español sigue siendo válido en Bélgica desde el punto de vista de una identificación o constatación de datos visual, por parte de una persona. Sin embargo, en el caso de la identidad electrónica no ocurre lo mismo puesto que los sistemas de identidad electrónica y de gestión de dicha identidad en cada país no son compatibles, es decir, no están preparados para interoperar. Surge por lo tanto uno de los principales problemas que nos ocupan, la interoperabilidad entre los sistemas de gestión de identidad a nivel pan-Europeo. De forma genérica podemos decir que dada la diversidad de sistemas de gestión de identidad, cuando un usuario de un sistema dado (ya sea un ciudadano, una empresa o la propia Administración) trata de comunicarse con Administraciones que se encuentran fuera del ámbito de su propio Sistema de Gestión de Identidad local surge la necesidad de comunicar los Sistemas de Gestión entre si y conseguir un entendimiento que permita que la identidad de un usuario de un sistema sea entendida y aceptada por el otro. Se hace necesario el establecimiento de un marco de

interoperabilidad a nivel de la Unión Europea para los Sistemas de Gestión de Identidad.

Con la intención de conseguir esto la Comunidad Europea adoptó el 25 de abril de 2006 su *eGoverment action plan* [6], en el que se realiza la siguiente afirmación:

> *The Commission, in cooperation with the Member States, will pursue policies to grant safe access to services EU wide. […] EU governments have agreed to facilitate this process by establishing secure systems for mutual recognition of national electronic identities for public administration web-sites and services. The Action Plan foresees a full implementation by 2010.*

Para conseguir establecer el marco de interoperabilidad la Unión Europea fijó un mapa de ruta [7]. En dicho mapa de ruta se establecen una serie de principios de diseño que se enuncian a continuación, todos 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:

- La usabilidad debe ser un aspecto dominante en el diseño de los sistemas.
- Cada estado miembro debe ser capaz de identificar a los usuarios dentro de sus fronteras.
- Cada estado miembro debe entregar a cada usuario los medios necesarios para identificarse y autenticarse a sí mismo electrónicamente.
- Con respecto a las autorizaciones de órdenes o representaciones, cada estado miembro debe proporcionar los medios para gestionar las competencias de los usuarios identificados dentro de sus fronteras.
- Cada estado miembro debe soportar mecanismos de validación online de identidades, competencias y órdenes.
- Entre los estados miembros se debe establecer un consenso a alto nivel respecto a la terminología en los Sistemas de Gestión de Identidad para garantizar la interoperabilidad semántica y conceptual.

A partir de los principios de diseño anteriores se derivan una serie de criterios sobre cómo debe ser un Sistema de Gestión de Identidad a nivel pan-Europeo:

- Federado. Debe existir una confianza mutua entre las distintas Administraciones en lo que se refiere a los métodos de identificación y autenticación.
- Multinivel. En el sentido de que se debe permitir a los Estados Miembros proporcionar múltiples niveles de seguridad para los servicios de gestión de identidad. Los requisitos de autenticación para cada servicio deben ser adaptados a las necesidades de seguridad de dicho servicio, lo que implica la definición a nivel Europeo de un conjunto de criterios para cada nivel de autenticación.
- Dependiente de fuentes fiables. Para garantizar la calidad de los datos debe existir, en cada Estado Miembro, una única fuente fiable para cada pieza de información correspondiente a una entidad registrada, de manera que se elimine la duplicidad de datos y se asegure una única fuente correcta y oficial.

- Permitir la incorporación del sector privado en aquellos Estados Miembros en los que se elija confiar en empresas privadas, por ejemplo instituciones financieras, para proporcionar servicios de gestión de identidad electrónica.

A pesar de la existencia del mapa de ruta, de los principios de diseño y los criterios comentados, 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 como veremos en el siguiente apartado se están proponiendo soluciones.

4 Análisis de las propuestas existentes hasta la fecha

Debido a los planes de acción lanzados por la Unión Europea, a lo largo de los últimos años han surgido iniciativas enfocadas a lograr la interoperabilidad entre los sistemas de gestión de identidad. La mayoría no pasan de ser propuestas teóricas que resuelven alguno de los problemas sin dar una solución completa, aunque algunas van más allá y proponen arquitecturas que se encuentran en la actualidad en fase de piloto. A continuación se comentan las más destacadas.

Quizá uno de los primeros estudios/proyectos dedicados a la interoperabilidad de los Sistemas de Gestión de Identidad fue el **Modinis eIDM Study** [8]. Dentro del modelo propuesto se llevó a cabo un estudio completo a alto nivel sobre el uso de los sistemas de gestión de identidad en los países miembros de la Unión Europea junto con un análisis de las principales consecuencias del uso de este tipo de sistemas de eIDM y un conjunto general de recomendaciones. Tras el estudio de los distintos perfiles nacionales, el estudio Modinis intentó definir un conjunto de aspectos clave para el despliegue de sistemas eIDM a escala europea. Su principal aportación a la interoperabilidad es la definición de una infraestructura de alto nivel, un modelo o marco conceptual, llamado Modinis Conceptual Framework, que es, fundamentalmente, un portal basado en federación que recoge las principales propuestas realizadas en el proyecto en cuanto a organización general y principios básicos que deben regir una infraestructura eIDM a nivel pan-Europeo. De forma resumida se puede decir que la infraestructura se basa en un modelo federado que confía en una serie de portales de identidad en cada Estado Miembro (al menos uno por estado, posiblemente más) que serían los responsables de la autenticación de una entidad a nivel nacional y de decidir el nivel de confianza que se otorga a los distintos procedimientos de autenticación realizados en cada Estado Miembro. En este modelo, los requisitos de autenticación para un servicio concreto en un determinado Estado Miembro aceptarían como equivalentes los niveles de autenticación y los mecanismos empleados en otro Estado en base a un conjunto de criterios, de manera que no sería necesario establecer ninguna infraestructura específica a nivel Europeo.

Como podemos ver, el modelo presentado constituye uno de los imaginables para un sistema pan-Europeo de Gestión de Identidad basado en un conjunto específico de conceptos centrales específicamente pensados para aplicaciones de *eGovernment*.

Otro sistema interesante de cara a dar solución a los sistemas de gestión de identidad es el denominado **TLS-Federation** [9].

Este proyecto tuvo como objetivo proporcionar un marco de trabajo regulatorio e interoperable para la gestión de identidad a nivel europeo. Se centró en el uso de tecnologías y estándares suficientemente conocidos y en la protección del lado del usuario frente a posibles escenarios de robo de identidad. El modelo TLS-Federation está basado en el uso de certificados durante el proceso de autenticación, lo que asegura la máxima seguridad para el proceso, y se construye sobre una aproximación centrada en el usuario, de manera que la identidad y los atributos de privacidad son gestionados directamente por él. El sistema está diseñado para ser usado en comunicaciones tanto entre sistemas dentro de un mismo país como entre distintos países. Cuando se compara TLS-Federation con otras posibles formas de llevar a cabo la gestión de identidad aparecen puntos prometedores, sobre todo a la hora de crear una infraestructura eficiente en costes. Es la única solución que no requiere, o requiere muy poca, instalación adicional y no hay necesidad de convertir las credenciales de sesión cuando se accede desde el dominio de cada estado miembro al dominio pan-Europeo.

La autenticación se lleva a cabo utilizando una implementación estándar de TLS y, en algunos casos, se puede utilizar como token de autenticación una I-Card (*Information Card*) [10]. Por otro lado, la implementación de TLS-Federation gira en torno a certificados basados en PKI y al uso de tarjetas inteligentes, por lo que se necesitan estándares adicionales como PKCS#11 y CSPs (*Cryptographic Service Providers*).

El aspecto central de TLS-Federation es la autenticación, estando menos desarrolladas la identificación y la autorización. En la actualidad, las investigaciones en curso han identificado dos vías diferentes para transportar atributos de usuario específicos de servicio, una de ellas se basa en el uso de certificados X.509 dinámicos, que pueden ser creados bajo demanda y de forma instantánea por un Proveedor de Identidad y que tienen un corto periodo de validez, y la otra se basa en la utilización de la tecnología I-Card.

Una I-Card es una pieza software que corresponde a una identidad digital de un usuario, es decir, es una colección de información de identidad de un usuario almacenada en un fichero. Al no ser información almacena en una tarjeta física, no está limitada en cuanto a longitud, tamaño y capacidad y puede copiarse fácilmente si se desea. Adicionalmente, una I-Card puede, en vez de almacenar directamente los datos de identidad de un usuario, contener punteros a una localización central desde donde pueden ser recuperados (es el caso por ejemplo de una tercera parte de confianza que gestione la información presente en las I-Card de los usuarios).

Si se pone en marcha un sistema de autenticación fuerte y el uso de proveedores de identidad gubernamentales basados en PKI comienza a ser un estándar de-facto en los Estados Miembros Europeos, entonces TLS-Federation se podría llegar a utilizar para la autenticación a nivel pan-Europeo. Independientemente de que esto último ocurra, los aspectos relativos a la autenticación en TLS-Federation deben ser tenidos en cuenta porque no necesitan, o necesitan una cantidad limitada de trabajo de integración. Cada parte de la tecnología ya existe y es soportada por la mayoría de los sistemas operativos, buscadores y servidores web existentes en el mercado actual. Es simplemente una cuestión de activarlo.

El proyecto **GUIDE** (*Creating a European Identity Management Architecture for eGovernment*) [11] tuvo como propósito fundamental el desarrollo de un modelo para

la interoperabilidad en materia de identidad en la Unión Europea tal que permita a los Estados Miembros de la Unión Europea (UE) fiarse de la identidad de una entidad (tanto ciudadanos como empresas) de otro Estado. El concepto básico subyacente en GUIDE es el de una Red Federada de Gestión de Identidad en la que los miembros, usuarios, Administraciones y empresas, alrededor de la Unión Europea puedan participar en los intercambios de información de identidad sin comprometer la privacidad y la seguridad de dicha información. Esto requiere de la afiliación de los miembros en círculos de confianza basados en acuerdos operacionales que definen las relaciones de confianza entre ellos. En otras palabras, un círculo de confianza es una federación de proveedores de servicios y proveedores de identidad que han establecido relaciones formales y acuerdos operacionales y con cuyos consumidores de servicios pueden llevar a cabo transacciones. Dentro del paisaje de la Unión Europea ya se han desarrollado varias de estas federaciones y círculos de confianza para distintos grupos de interés, tanto administrativos como comerciales. En particular, muchos Estados Miembros están involucrados en el desarrollo de dichas federaciones a nivel nacional. Sin embargo, en muchos casos estas federaciones se han constituido o están siendo constituidas de forma aislada unas de las otras. El objetivo de GUIDE ha sido el de definir una arquitectura que permita la unión de dichas federaciones en un gran círculo de confianza con la intención de facilitar un entorno de identidad aparentemente único a lo largo de toda la Unión Europea. Esto es un prerrequisito anterior a que cualquier identidad pueda ser intercambiada de forma segura entre Estados Miembros. A este respecto GUIDE está concebido como una federación pan-Europea de federaciones de identidad que puede ser descrita también como una red de identidad. La esencia de esto es la provisión de un canal de confianza entre Estados Miembros para la realización de transacciones relacionadas con la identidad.

Otra propuesta de sistema de Gestión de Identidad a nivel pan-Europeo es **STORK** (*Secure idenTity acrOss boRders linKed*) [12]. Este proyecto, recientemente iniciado, trata de desarrollar y probar especificaciones comunes para un reconocimiento mutuo y seguro de las identidades electrónicas (eID) nacionales de los países participantes. Como objetivos concretos podemos encontrar el definir modelos y especificaciones comunes para el mutuo reconocimiento de eIDs entre países, probar en un entorno real soluciones de eID seguras y fáciles de utilizar tanto para ciudadanos como empresas e interactuar con otras iniciativas de la Unión Europea para maximizar la utilidad de los servicios de eID. Para conseguir lo anterior el modelo que STORK propone se basa en estudios previos realizados por IDABC [13] que describen, a alto nivel, un modelo federado para interoperabilidad, tecnológicamente neutral y que soporta múltiples niveles de autenticación. Concretamente, se presenta un modelo que confía en un proxy y requiere de la creación de proveedores de identidad a nivel nacional (al menos uno por país). Este sistema de proveedores de identidad se une en STORK a una red de proxys proveedores de servicios denominados PEPS (*Pan European Proxy Services*). Estos proxys serán creados a nivel nacional, aunque el modelo también contempla la posibilidad de que exista un proxy europeo centralizado o incluso un modelo mixto, de tal modo que ciertos países confían en un PEPS nacional mientras que otros lo hacen en un PEPS Europeo. Los PEPS sirven básicamente para superar el problema técnico que se presenta cuando aparece un conjunto amplio de soluciones de identificación/autorización, como es el caso del

escenario europeo. Por ejemplo, en algunos casos un ciudadano puede querer utilizar una combinación nombre de usuario-contraseña para acceder a un servicio mientras que otro pretende utilizar su tarjeta de identificación electrónica. Suponiendo que el dueño de la aplicación dé por buenos ambos métodos de identificación, la infraestructura técnica debe ser capaz de soportar ambas soluciones. Es aquí donde entra en escena el PEPS, cuya principal función es la de conectar los proveedores de servicios con los proveedores de identidad adecuados en cada país y validar la confianza y la seguridad de la información de identidad enviada por los proveedores de identidad. Por lo tanto, el conjunto de PEPS formaría un círculo de confianza en el sentido de, por ejemplo, las soluciones indicadas por Liberty Alliance [3]. Para el transporte de atributos de identidad desde los proveedores de identidad a los proveedores de servicio a través de los PEPS se sugiere el uso de asertos SAML. En lo referente al marco tecnológico elegido para interconectar las soluciones o el modelo conceptual detrás del marco de trabajo las decisiones no se han hecho públicas aún. Sin embargo, dentro de las intenciones del proyecto STORK se encuentra el ser lo más tecnológicamente transparente posible y el asegurar soluciones interoperables con los sistemas nacionales de eID existentes. Así mismo, STORK intenta confiar tanto como sea posible en estándares abiertos.

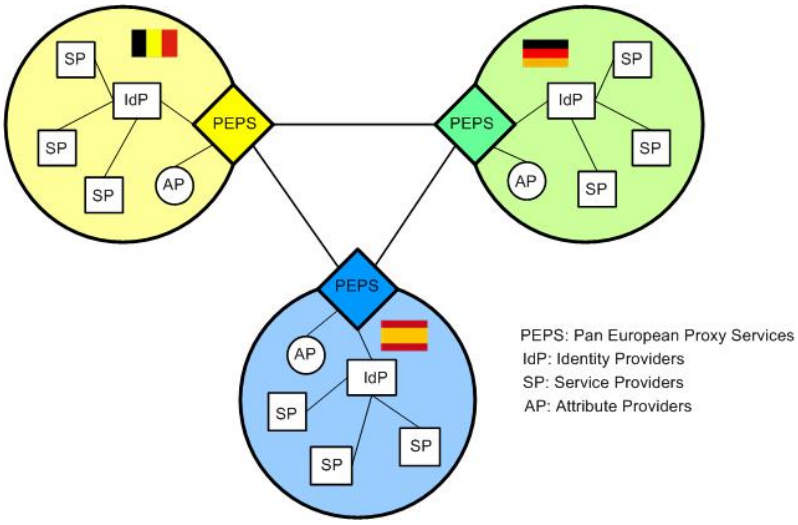

Fig. 1. Esquema de la arquitectura propuesta en el proyecto STORK

Tras un estudio pormenorizado de estos proyectos europeos, se ha realizado un análisis e identificación de las tendencias actuales en cuanto a los sistemas de gestión de identidad así como de las carencias y problemas que presentan.

Parece claro que, a día de hoy, los sistemas de gestión de identidad están orientados hacia la federación y el multinivel. Esta orientación no es ni mucho menos extraña si tenemos en cuenta que estos dos aspectos se derivaban directamente de los principios de diseño establecidos en el mapa de ruta europeo [7] tal y como vimos en el apartado 3.

Si se analiza el estado actual tanto desde el punto de vista de legislación como de implantación de sistemas de gestión de identidad en los distintos países miembros de la Unión Europea aparecen claras diferencias, existiendo países en los que la eID y el eIDM están claramente implantados y otros en los que todavía se está comenzando. No es válida por lo tanto una aproximación a la implantación de un sistema de gestión de identidad único y global, puesto que no todos los países parten del mismo punto y cada país presenta sus peculiaridades en cuanto al tratamiento de los datos y a la relación con los ciudadanos.

Un sistema federado que permita constituir un círculo de confianza entre las infraestructuras de todos los países miembros y que permita una fácil incorporación de futuros países se presenta como una buena solución, ya que permite la creación de la infraestructura pan-Europea sin apenas modificar lo ya implantado. Soluciones como la presentada en Modinis, basada en la existencia de portales de identidad en cada país encargados de la autenticación interna y la gestión de las confianzas depositadas en los sistemas de gestión de otros países, o la de STORK, centrada en el uso de proxys de acceso a servicios en cada país, se adaptan perfectamente a la federación y a la idea de mantener lo más intacto posible el sistema ya implantado en cada estado miembro.

Por otro lado, la heterogeneidad de los sistemas existentes y de los mecanismos de autenticación/autorización presentes en cada país, hace que sea fundamental dotar a un sistema de gestión de identidad pan-Europeo de la capacidad de mapear tokens de identidad entregados por el sistema de gestión de identidad de un país a sus equivalentes en otro si se pretende un acceso a los servicios lo más transparente posible por parte de los ciudadanos y usuarios en general. Esto se traduce en que el sistema debe ser necesariamente multinivel. Varios de los proyectos presentados cumplen con este criterio.

Otra de las tendencias detectadas es la utilización de estándares, concretamente la utilización de SAML, para el intercambio de tokens de autenticación entre sistemas de gestión de identidad. Muchos de los proyectos analizados, como por ejemplo STORK y GUIDE, se basan en el uso de SAML, llegando GUIDE a proponer modificaciones en el estándar para adaptarlo a su modelo. Evidentemente la utilización de soluciones estándar siempre es beneficiosa, pero antes de tomar una decisión clara se debe analizar la problemática y tratar de buscar la solución más adecuada. Una vez elegida una solución, se debe justificar su elección y dar solución a los problemas que se puedan derivar de la misma. Ninguno de los proyectos estudiados presenta un análisis claro y una justificación de la elección de SAML, adoleciendo por lo tanto de los problemas derivados del uso del mismo. Por ejemplo, STORK se basa en el uso de SAML para el intercambio de información entre sus PEPS y sufre, como consecuencia de ello, de la posibilidad de ataques del tipo *man-in-the-middle*. Aunque la tendencia actual es hacia la utilización de SAML, ésta presenta ciertos problemas y soluciones alternativas como la utilización de certificados X.509, generados de forma dinámica, propuesta por proyectos como TLS-Federation, deben ser tenidas en cuenta y evaluadas antes de tomar una decisión definitiva.

Además de las tendencias, se han identificado en los proyectos analizados diferentes problemas que se podrían considerar comunes a todos ellos. El primero aparece en la gestión de la información, concretamente en la fiabilidad y calidad de los datos manejados. Normalmente, en los sistemas de gestión de identidad actuales

no existe una única fuente de datos y esto puede dar lugar a problemas de duplicidad e incoherencias. De acuerdo al mapa de ruta, se debe disponer en cada país de una única fuente fiable para cada pieza de información correspondiente a una entidad registrada, de manera que se elimine la duplicidad de datos y se asegure que éstos son correctos y oficiales. Sólo el proyecto STORK considera la existencia de estas fuentes a través de los proveedores de atributos de cada país.

Por otra parte, todos los proyectos analizados presentan soluciones a la gestión de identidad a nivel pan-Europeo muy centradas en el entorno de la Administración Electrónica, del eGovernment. No se presenta en ninguno de los proyectos un estudio sobre la posibilidad de interoperabilidad con el entorno privado, ya sea como proveedores de infraestructura para la gestión de identidad o como proveedores de servicios, por ejemplo, un banco que permita el uso de la tarjeta de identificación electrónica para el acceso seguro a la aplicación de banca electrónica por parte de los usuarios. Esto se produce a pesar de que el mapa de ruta establece que el desarrollo de aplicaciones del sector privado que se apoyen en la infraestructura de gestión de identidad pública serán aspectos muy a tener en cuenta para facilitar e incrementar la aceptación y el atractivo de los sistemas de identificación electrónica por parte de los usuarios.

Finalmente, un problema común a todos los sistemas propuestos para la gestión de identidad, tanto a nivel nacional como a nivel pan-Europeo, es el de la delegación de identidad, la delegación de autorización y el manejo de roles. Muchas transacciones son realizadas a día de hoy por representantes legales autorizados a operar en nuestro nombre. Por ejemplo, en España un ciudadano puede autorizar a otra persona, típicamente a través de una Oficina Gestora, a realizar todos los trámites relativos a la presentación de impuestos anuales con la Administración. Así mismo, un ciudadano puede tener distintos roles de forma simultánea dentro del sistema de gestión de identidad, siendo a la vez ciudadano y representante legal de una empresa u organización. Los sistemas de gestión de identidad propuestos hasta la actualidad han hecho muy pocos progresos en estos aspectos y ninguno da un soporte completo al manejo de roles y delegaciones.

5 Propuesta de infraestructura de interoperabilidad

Dentro del mencionado proyecto de investigación en el que trabaja este grupo se ha analizado la problemática de la gestión de identidad en todos los niveles de la Administración Pública, desde el entorno local al pan-Europeo. Tras un estudio pormenorizado de dichos niveles se llegó a la conclusión de que los problemas de interoperabilidad que aparecen entre distintos países miembros de la Unión Europea en cuanto a gestión de identidad, aparecen en la interacción entre los distintos niveles de la Administración, incluso dentro del mismo país como por ejemplo España. La intención del grupo de investigación, y concretamente de los autores de este artículo, es proponer un modelo de interoperabilidad que pueda ser aplicado no solo a nivel pan-Europeo, sino también a nivel nacional, autonómico y local, de tal forma que la interoperabilidad en la gestión de la identidad esté garantizada en todos los niveles. El modelo toma como puntos de partida las ventajas identificadas en los sistemas de

gestión de identidad presentadas en el apartado anterior y pretende, adicionalmente, solucionar los problemas identificados.

A día de hoy podemos decir que el sistema estará basado en la federación, conseguida mediante el establecimiento de círculos de confianza en cada uno de los niveles y entre niveles, tal como se presenta en la figura 2. En dicha figura se puede apreciar cómo en cada uno de los niveles de la Administración (local, autonómico y nacional) se establece un círculo de confianza que agrupa a uno o varios Proveedores de Identidad (IdP) y Proveedores de Servicios (SP) en ese nivel. En lo que se refiere a la autenticación se hará uso del mapeo de tokens, es decir, se permitirá el mantenimiento de los sistemas ya establecidos de manera que los elementos de autenticación en uso serán mapeados a elementos comunes que garanticen la interoperabilidad. Para ello se adopta el concepto de proxy como interfaz entre los sistemas de gestión de identidad, de manera que garantizarán la interoperabilidad tanto dentro de un mismo nivel (por ejemplo la local entre dos ayuntamientos) como entre niveles (por ejemplo entre un ayuntamiento y su comunidad autónoma). Para el intercambio de tokens de autenticación se utilizarán los certificados X.509. Concretamente se utilizarán certificados generados de forma dinámica y se explotarán las capacidades de las extensiones, lo que nos ofrecerá la posibilidad, por ejemplo, de llevar a cabo la implantación de servicios con delegación de identidad y manejo de roles, hasta ahora apenas considerados en las arquitecturas propuestas.

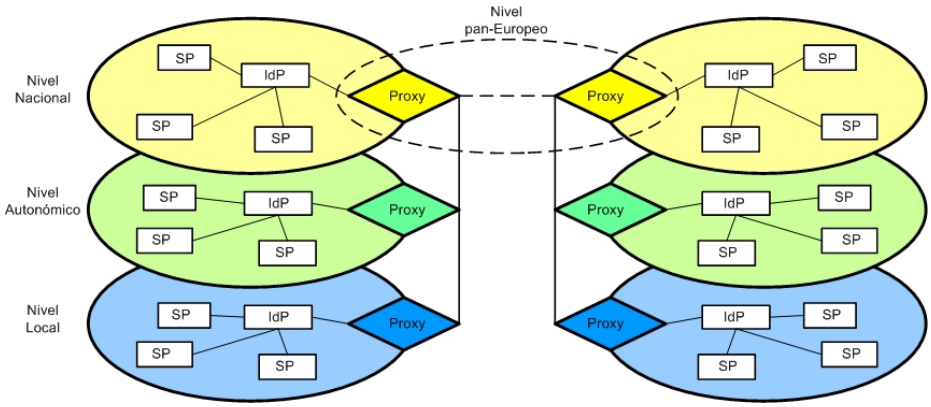

Fig. 2. Infraestructura propuesta

Por último, un problema aún en estudio en la propuesta es el de garantizar la unicidad y evitar incoherencias y duplicidad de datos. La intención es establecer fuentes de datos únicas en cada nivel y sincronizadas entre niveles, pero esto último presenta una serie de dificultades derivadas del hecho de que una misma entidad puede estar presente en distintos niveles y con datos que, a pesar de ser verdaderos, no guardan una relación directa, por lo que aparecen problemas a la hora de garantizar la sincronización.

En la actualidad se ha iniciado la implementación de un piloto de la infraestructura propuesta en el Ayuntamiento de Mejorada (Madrid), con la intención de demostrar la viabilidad de la solución y las posibilidades de la misma. En esta experiencia piloto se

implementa en un escenario real y, a escala reducida, un círculo de confianza con varios Proveedores de Servicios (SP) y un Proveedor de Identidad (IdP), empleando las herramientas ofrecidas por Shibboleth [14]. Para ello, se han seleccionado varios servicios telemáticos que próximamente proporcionará el ayuntamiento a través de Internet: solicitud de bonificaciones y exenciones tributarias, solicitud de autorizaciones (instalación de quioscos, terrazas, bares en la vía pública, grúas, etc.) y solicitud de licencias de actividad, de manera que cada uno de estos servicios se ofrece a través de un Proveedor de Servicios distinto, pero todos ellos dentro del mismo círculo de confianza. Para el acceso a estos servicios se contempla que la identificación de los ciudadanos se realice a través de un certificado digital X.509 integrado en el Documento Nacional de Identidad (eDNI) o emitido por una Autoridad de Certificación aceptada para operar dentro de la Administración española. La verificación de la identidad de los ciudadanos se lleva a cabo a través del Proveedor de Identidad de ese círculo de confianza, de manera que un ciudadano una vez autenticado para acceder a un servicio puede acceder a otro servicio del mismo círculo. Una vez creado el círculo de confianza se trabaja en la definición del proxy que se encargará del mapeo de tokens y permitirá que el Proveedor de Identidad pueda admitir como válidas identidades procedentes de otros Proveedores, de manera que se pueda probar la viabilidad de las soluciones propuestas.

7 Conclusiones

La búsqueda de soluciones a los problemas de interoperabilidad en la gestión de identidad es un tema muy importante que, sin duda, contribuirá a facilitar la vida a los ciudadanos en un mundo globalizado. Sin embargo, parece claro que estas soluciones no deberían obligar a modificar los esquemas nacionales de identificación digital desarrollados por cada país conforme a sus necesidades y legislación específicas, pero sí deberían ser lo suficientemente fiables y robustos para ser aceptados mayoritariamente por todos los países del entorno, en nuestro caso de Europa.

Aunque la UE ha puesto en marcha distintas iniciativas para buscar una solución a este problema creciente, a día de hoy existen importantes aspectos por resolver como la falta de integración de las soluciones con el sector privado, la ausencia de fuentes de datos únicas que garanticen la unicidad y coherencia de la información relativa a las entidades o los problemas derivados de la utilización de determinados estándares.

En esta línea, el proyecto de investigación que en la actualidad realiza este grupo está orientado a buscar solución a estos problemas bajo dos vertientes distintas. Por una parte, se pretende que las soluciones propuestas tengan eco a nivel europeo, para ello se mantiene contacto regular con los principales grupos que trabajan en este tema. Por otra, se busca extrapolar las soluciones planteadas al entorno de la Administración española, donde los problemas de interoperabilidad entre los sistemas de gestión de identidad en los distintos niveles de la Administración son semejantes a los existentes a nivel europeo. Con todo ello, se pretende realizar aportaciones que contribuyan a avanzar hacia una interoperabilidad total en la gestión de identidad, tanto a nivel nacional como pan-europeo, que permita una provisión de servicios sencilla y totalmente transparente para el usuario.

Bibliografía

1. Independent Centre for Privacy Protection; Unabhängiges Landeszentrum für Datenschutz; Schleswig-Holstein; Studio Notarile Genghini; Identity Management Systems (IMS): Identification and Comparison Study, http://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf (2003).
2. Parlamento Europeo y Consejo de la Unión Europea: 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, vol. L, 281, pp. 31-50. Luxemburgo: Unión Europea (23 de Noviembre de 1995).
3. Liberty Alliance Project, http://www.projectliberty.org.
4. Wason, T.: Liberty ID-FF Architecture Overview. Version: 1.2-errata-v1.0. Liberty Alliance Project (2005), http://www.projectliberty.org/liberty/content/download/318/2366/file/draft-liberty-idff-arch-overview-1.2-errata-v1.0.pdf.
5. The Modinis IDM Study Team: Modinis Study on Identity Management in eGovernment: Common Terminological Framework for Interoperable Electronic Identity Management. Version 2.01. eGovernment Unit, DG Information Society and Media, European Commission (23 de Noviembre de 2005), https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc.
6. Varios: eGovernment: Commission calls for ambitious objectives in the EU for 2010. Bruselas (25 de Abril de 2006), http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/523&format=PDF&aged=1&language=EN&guiLanguage=en.
7. Varios: A Roadmap for a pan-European eIDM Framework by 2010. Version 1.0. European Commission, Information Society and Media Directorate-General, eGovernment Unit, http://ec.europa.eu/information_society/activities/egovernment/docs/pdf/eidm_roadmap_paper.pdf.
8. ModinisIDM, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome.
9. Bruegger, B. P., Hühnlein, D., Schwenk, J.: TLS-Federation - a Secure and Relying-Party-Friendly Approach for Federated Identity Management. http://porvoo14.dvla.gov.uk/documents/tls_federation_final.pdf.
10. Microsoft Corporation. A technical reference for InfoCard v1.0 in Windows (Agosto 2005), http://download.microsoft.com/download/5/4/0/54091e0b-464c-4961-a934-d47f91b66228/infocard-techref-beta2-published.pdf.
11. GUIDE, Creating a European Identity Management Architecture for eGovernment, http://istrg.som.surrey.ac.uk/projects/guide/overview.html.
12. STORK, Secure idenTity acrOss boRders linked, http://www.eid-stork.eu/.
13. Majava, J. and Graux, H.: Common Specifications for eID interoperability in the eGovernment context. IDABC European eGovernment Services (Diciembre 2007), http://ec.europa.eu/idabc/servlets/Doc?id=30989.
14. Shibboleth, http://shibboleth.internet2.edu/.