El DNIe español como puerta de entrada a servicios de Administración electrónica en Europa: Proyecto STORK



Miguel Álvarez Rodríguez,

Jefe de Área de Cooperación en T.I.
Dirección General de Modernización Administrativa, Procedimientos y para el impulso de la Administración electrónica
Ministerio de Hacienda y Administraciones Públicas

1 INTRODUCCIÓN 3

2 ¿CUÁL ES EL ORIGEN DEL PROYECTO? 3

3 INICIATIVAS EUROPEAS EN MATERIA DE GESTIÓN DE IDENTIDADES ELECTRÓNICAS 4

4 PROYECTO STORK 5

***5* ARQUITECTURA DE LA PLATAFORMA DE INTEROPERABILIDAD DE STORK 6**

6 CONCLUSIONES 10

7 ACRÓNIMOS UTILIZADOS: 11

1 Introducción

El proyecto europeo **STORK** (**S**ecure iden**T**ity acr**O**ss boRders lin**K**ed) pretende establecer una plataforma de interoperabilidad y reconocimiento mutuo transfronterizo de las identidades electrónicas existentes en cada Estado Europeo, lo cual **permitirá a los ciudadanos acceder e identificarse en servicios de administración electrónico de otros país europeo, a través del uso de sus DNIe o identidades electrónicas nacionales**. Es posiblemente el mayor proyecto Europeo en materia de identidad electrónica que existe hoy en día en el ámbito del sector público. Para España **supondrá la aceptación de los certificados digitales españoles, como los del DNI electrónico en servicios de Administración electrónica de otros países**, lo cual facilitará la relación de nuestros ciudadanos y empresas con otras AAPP europeas.

Después de la pruebas o pilotos que se van a llevar a cabo en STORK donde se probará dicha plataforma de interoperabilidad con ciudadanos reales, estaría a disposición de la AAPP europeas una plataforma de interoperabilidad que permitiría la identificación segura de los ciudadanos a través de sus identidades electrónicas de manera transparente y sencilla a través del intercambio de aserciones de identidad SAML, sin necesidad de que cada aplicación tengan que lidiar con la complejidad técnica de aceptar diferentes tipos de identidades electrónicas de muchos países (múltiples tarjetas, drivers y certificados electrónicos). **La plataforma** además de permitir identificar de manera segura a los ciudadanos, **permite el intercambio de todos los datos de identidad y atributos** que sean necesarios por parte de una aplicación, para completar un proceso de registro o autenticación por parte de un ciudadano.

La Plataforma de interoperabilidad, pionera en Europa, se ha diseñado con una arquitectura totalmente distribuida con dos principios fundamentales: el máximo control del usuario sobre sus datos (user centric approach) y la garantía de privacidad. La solución desarrollada propone el uso del estándar **OASIS SAML 2.0** como mecanismo para el intercambio de los datos de identidad de los ciudadanos. El consorcio del proyecto STORK lo forman 29 entidades de 14 países, entre las cuales el Ministerio de Hacienda y Administraciones Públicas español, que es el líder de uno de los paquetes de trabajo más relevantes.

2 ¿Cuál es el origen del proyecto?

Aunque el uso de la identidad electrónica está extendiéndose de forma generalizada en los servicios telemáticos tanto del sector público como del privado, en España fundamentalmente a través del uso DNIe y otros certificados electrónicos, y se ha convertido en unos de los motores y facilitadores de servicios de administración electrónica seguros, aún no está resuelta la interoperabilidad de dichos elementos a nivel internacional.

De hecho, podemos plantearnos las siguientes cuestiones:

–¿Puede usar un ciudadano español su flamante DNI electrónico para autenticarse ante un Servicio Público electrónico belga?

–De la misma manera, puede un ciudadano belga residente en España utilizar su DNIe nacional como medio de identificación ante una aplicación de Administración electrónica española?

Actualmente disponemos de 'silos' de identificación y firma electrónica a nivel nacional. Cada organización tiene sus mecanismos de identificación electrónica propios y en muchos casos no son compartidos con otros departamentos o usuarios.

Pensemos en la problemática de la gestión de la identidad electrónica a nivel europeo con 27 estados miembros, cada uno con su propia idiosincrasia y diferentes avances en materia de identificación electrónica:

- los países anglosajones utilizan de forma masiva técnicas de autenticación menos seguras y livianas como usuario y password, sin desarrollar de manera plena la identificación basada en certificados electrónicos reconocidos.

- la mayoría de los países europeos ya empiezan a implantar certificados digitales basados en soluciones de PKI (el 75% de los países europeos ya tienen desplegados soluciones de PKI mas o menos extendidas según el Informe de IDABC de la Comisión Europea sobre Diferencias y Similitudes en materia de eID).

- Un puñado pequeño de países están en la vanguardia de la identificación electrónica al emitir tarjetas nacionales criptográficas que incluyen la firma reconocida y la autenticación más fuerte basada en certificados digitales sobre un soporte de dispositivo seguro de creación de firma con chip: España con nuestro DNI electrónico, o Alemania, Austria, Bélgica, Finlandia, Estonia, Portugal y Suecia.

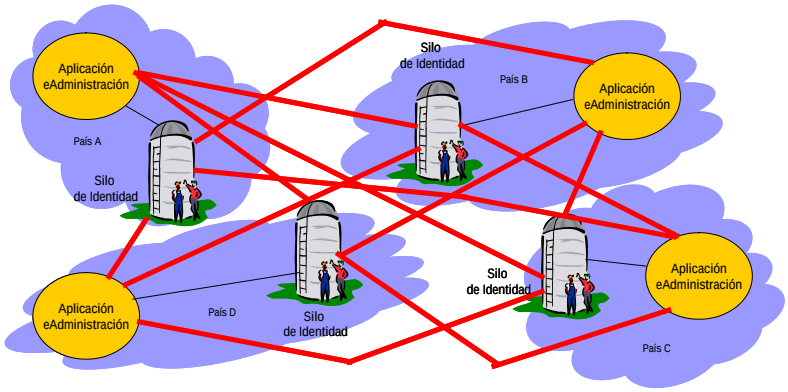


Figura 1. Silos de identidades electrónica

3 Iniciativas europeas en materia de gestión de identidades electrónicas

La identidad electrónica está considerada desde hace años como una de las piezas esenciales para favorecer la prestación de servicios electrónicos seguros.

De hecho, el plan de acción "i2010 – La Sociedad de la Información y los Medios de Comunicación al Servicio del Crecimiento y el Empleo" fue lanzado por la Comisión Europea en Junio de 2005 como un marco para cubrir los retos y desarrollos de la sociedad de la información en Europa hasta el año 2010. Esta iniciativa promueve una economía digital competitiva y abierta, posicionando a las Tecnologías de la Información y las Comunicaciones como el hilo conductor del cambio. Propone la administración electrónica como una de las áreas específicas cuyo Plan de Acción se centra en la modernización de las Administraciones

europeas para que los ciudadanos accedan a sus servicios de forma telemática. En este plan ya se reasalta la necesidad de avanzar en materia del reconocimiento de las identidades electrónicas europeas.

Además, en la última declaración Ministerial sobre administración electrónica que fue acordada en Malmö (Suecia) en el 2009, se destaca la necesidad de identificar las áreas o aspectos claves en los que se tiene que trabajar para conseguir la ansiada interoperabilidad transfronteriza en administración electrónica. Entre las áreas claves se resalta el reconocimiento de la identidad y la firma electrónica entre los estados miembros.

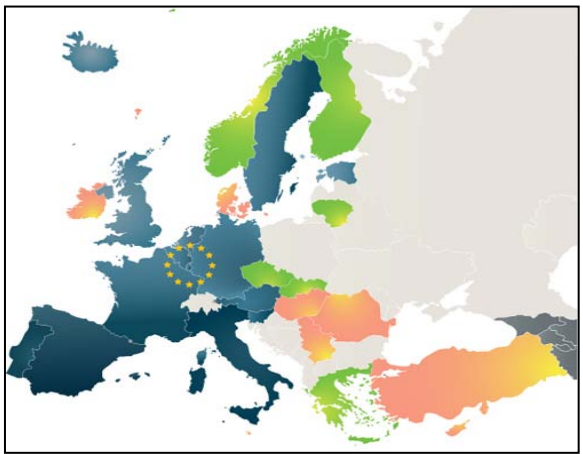
Por otro lado, el programa de la **Comisión Europea sobre Innovación y Competitividad (CIP)** dentro del Plan de acción Europeo i2010 define tres programas plurianuales en el periodo 2007-2013, entre los que se encuentra el programa base sobre políticas TIC, " The Information and Communication Policy Support Programme" (**ICT PSP**) que se centra en estimular la innovación y la competitividad a través de un mejor uso de las TIC por los ciudadanos, gobiernos, empresas y en particular las Pymes.Dentro de las acciones definidas en este programa se encuentra el desarrollo de Servicios de Administración Electrónica eficientes, interoperables y seguros. El Objetivo 1.2 de esta acción persigue el reconocimiento paneuropeo de las identidades electrónicas (eID) de manera transfronteriza, lo que se traduce la implementación de unos sistemas y unas especificaciones técnicas comunes en toda Europa para el reconocimiento de las diferentes eID y la autenticación electrónica, lo cual posibilitará a los ciudadanos, empresas y funcionarios el uso de sus identidades electrónicas nacionales en cualquier Estado Miembro de una manera segura.

4 Proyecto STORK

Como consecuencia del programa CIP, en el año 2008 se constituyó un Consocio denominado STORK compuesto por AA.PP. pertenecientes de 14 países europeos, entre ellos España para la realización de piloto pruebas de interoperabilidad y otras actividades complementarias relativas a la gestión europea de las identidades electrónicas.

Figura 2. Marca corporativa del proyecto

El objetivo del proyecto STORK (Secure idenTity acrOss boRders linKed) es precisamente crear una plataforma pan-europea para el reconocimiento mutuo de las identidades electrónicas existentes en Europa. De esta forma, los ciudadanos europeos podrán realizar empleando su identidad electrónica nacional.



El proyecto dispone de un presupuesto aproximado de 20 millones de euros, de los cuales la Comisión Europea subvenciona la mitad. El proyecto se enmarca en el programa CIP

(Competitiveness and Innovation Programme), más concretamente en ICT-PSP (ICT Policy Support Programme). El Consorcio del proyecto lo forman actualmente 29 entidades, incluyendo gobiernos de **14 países diferentes** (color azul en el mapa), y está actualmente en marcha una nueva ampliación del proyecto a **5 nuevos estados** (en color verde en el mapa).

El Ministerio de Hacienda y Administraciones Públicas español lidera el paquete de trabajo donde se define e implementa la plataforma de interoperabilidad. La unión de los esfuerzos e intereses de todos los socios participantes, que abarcan las Administración Públicas europeas, la industria y el mundo académico, asegura el máximo alcance e impacto de los resultados que se obtengan.

En concreto, uno de los resultados del proyecto STORK será el despliegue de una serie de **pilotos** que permitirán probar en un entorno real las capacidades de la plataforma de interoperabilidad desarrollada, entre los que cabe mencionar:

- Cross-border authentication, en el cual se pretende demostrar que una serie de servicios seleccionados pueden ser accedidos desde diferentes Estados Miembro.
- SaferChat, el cual desarrolla un entorno de mensajería instantánea seguro accesible a los usuarios mediante la autenticación con su identidad electrónica.
- **Movilidad de estudiantes**, cuyo principal objetivo es permitir la movilidad de estudiantes en toda Europa al facilitar la autenticación, con su identidad electrónica nacional, a la hora de realizar los trámites con la Universidad destino.
- eID Electronic delivery, piloto que permitirá implantar un servicio de entrega electrónica de documentos basada en las infraestructuras nacionales.
- **Cambio de domicilio transfronterizo**, el cual se centrará en un servicio de cambio de domicilio de un país a otro, accesible mediante la identidad electrónica del país origen.

El Ministerio de Hacienda y Administraciones Públicas participa en los pilotos de movilidad de estudiantes en colaboración con la **CRUE** (Conferencia de Rectores de Universidades Españolas) y en el de cambio de domicilio. Asimismo, lidera la parte del proyecto encargada de definir la arquitectura y las especificaciones comunes de interoperabilidad que permitan integran las identidades electrónicas de los países participantes, o dicho de otra manera, la plataforma de interoperabilidad que cada país debe construir.

El proyecto se encuentra en su fase de implementación de la plataforma. Para mitad de este año se prevé poner en funcionamiento los diferentes pilotos anteriormente mencionados para que puedan ser utilizarlos por ciudadanos reales.

5 Arquitectura de la plataforma de interoperabilidad de STORK

Actualmente existe gran diversidad de soluciones de eID desplegadas o en proceso de implantación en cada uno de los países participantes.

Con el objetivo de evitar la modificación de las infraestructuras nacionales implicadas, se ha desarrollado un modelo común de medición de los niveles de aseguramiento de las posibles identidades electrónicas que existen en Europa, denominado STORK QAA (Quality Authentication Assurance). Este modelo define cuatro niveles QAA para las soluciones eID. A mayor nivel, mayor garantía en la identidad debe proporcionar la solución eID, y por tanto mayores requisitos debe cumplir. Para la definición de los niveles se ha tenido en cuenta tanto la componente organizativa como técnica de cada solución. Los niveles QAA definidos son similares a los descritos por IDABC, y compatibles con los definidos en el marco de trabajo de aseguramiento de las identidades electrónicas de Liberty. Por ejemplo, el nivel de aseguramiento o QAA mas bajo correspondería a soluciones de identificación electrónica

basadas en usuario y password, mientras que el máximo nivel sería a través de certificado electrónico en un DNI electrónico o smart-card.

Por otra parte, cada país define, de acuerdo a su marco legislativo y criterio nacional, los niveles de garantía o aseguramiento de las soluciones eID que operan en sus fronteras. España básicamente acepta certificados electrónicos como mecanismos de identificación electrónica, que corresponderían con u nivel 3 o 4 en STORK. Por ello el modelo STORK QAA realiza un mapeo de los niveles existentes en cada país a los niveles comunes de aseguramiento de las eIDs definido por el STORK QAA, de forma que se puede realizar una traducción de un nivel nacional a otro dentro de un marco de interoperabilidad común.

Cuando el acceso a un servicio ofrecido por un Proveedor de Servicios (SP, Service Provider) requiere que el usuario se autentique, es necesaria una infraestructura de identidad digital para la emisión y posterior verificación de las credenciales necesarias.

Un Proveedores de Identidad (IdP, Identity Provider) es la entidad que proporciona, con unas determinadas garantías, una identidad electrónica al usuario final, y que le permiten autenticarse en los SPs. Esta entidad también se encarga de validar la identidad cuando un SP o tercera parte (relying party) así lo requiere.

El servicio de autenticación de STORK permite a un Estado Miembro delegar la autenticación de un usuario en el país que emitió su identidad electrónica. De esta forma, STORK permite a cualquier SP obtener, de forma transparente, una evidencia digital de la identidad del usuario que desea acceder al servicio, independientemente del país al que pertenezca. Esta evidencia es proporcionada por el IdP del país origen que emitió la identidad al usuario.

Para permitir el diálogo entre los diferentes Estados Miembro (MS), se desplegará en cada país una entidad llamada PEPS (Pan-European Proxy Service) que integra las funcionalidades específicas de STORK. La siguiente figura muestra la arquitectura distribuida diseñada.

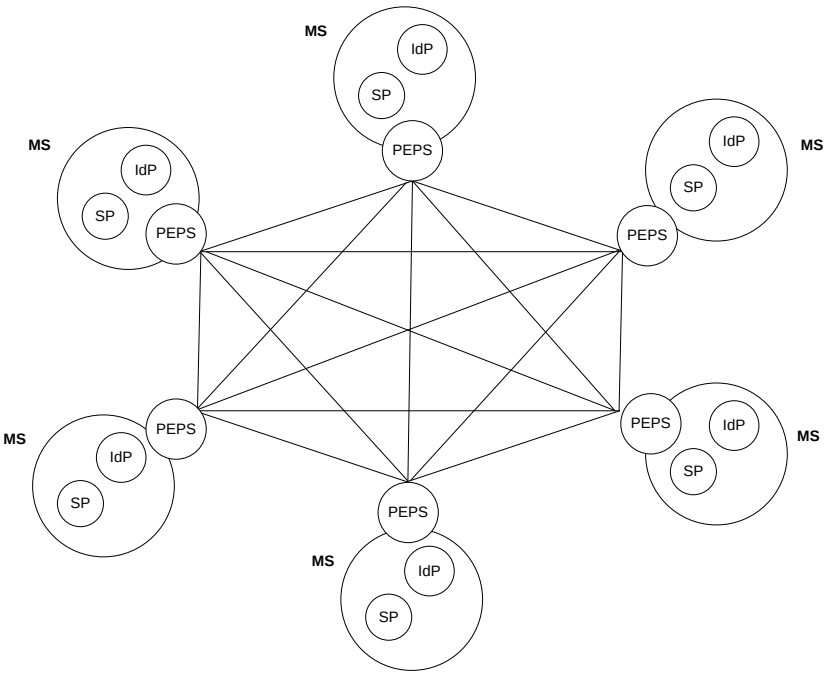


Figura 3. Arquitectura de interoperabilidad de STORK

Como puede observarse en la figura anterior, las comunicaciones se producen entre todos los PEPS, generando una arquitectura distribuida en malla. Cada PEPS dispone de una parte común para todos los países participantes, y de una parte específica que implementará cada país y aglutinará sus singularidades particulares y concretas, como por ejemplo las interacciones con sus SPs e IdPs. La siguiente figura muestra de forma más detallada la comunicación que se produce entre todos los actores implicados.

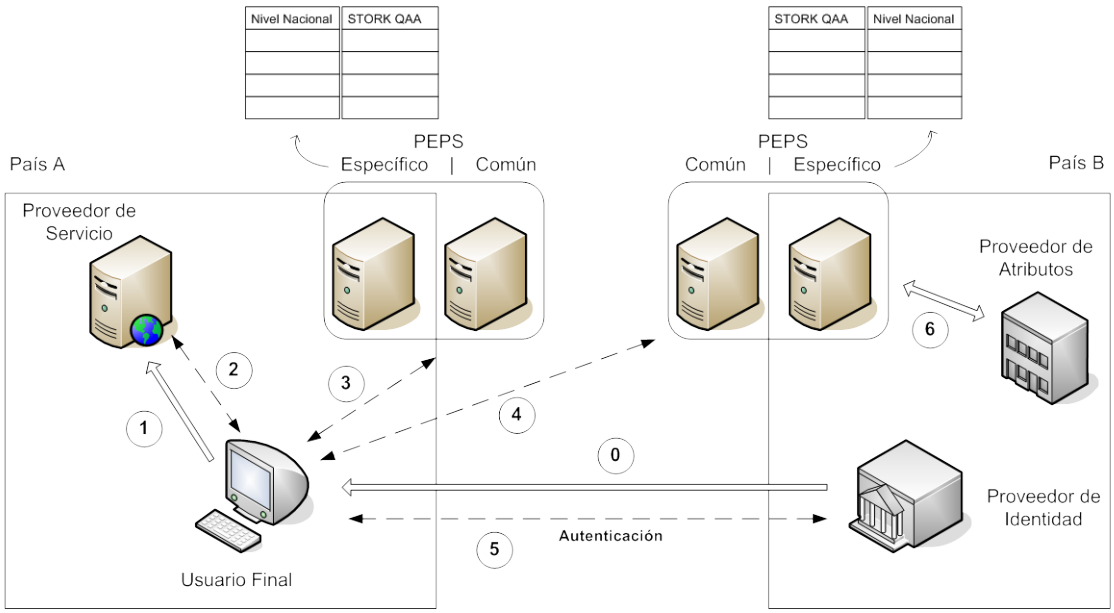


Figura 4. Arquitectura detallada para el Servicio de Autenticación

Un usuario desea acceder a un servicio ofrecido por cierto SP, en el país A (1), y dispone de una solución eID emitida por un IdP del país B (0). El servicio obliga al usuario a autenticarse, siendo el proveedor quien decide qué nivel de aseguramiento del eID se requiere. Dicho nivel estará en consonancia con los niveles nacionales, y será el PEPS del país A el encargado de mapearlo al nivel QAA.

El SP redirigirá al usuario al PEPS del país A con el fin de gestionar su autenticación (2 y 3). El PEPS detectará el país de origen del usuario, remitiéndolo al PEPS correspondiente (4). El PEPS del país origen redirigirá a su vez al usuario para que se autentique contra el IdP que emitió su identidad electrónica (5). En el ejemplo asumimos que dicha identidad cumple con el nivel de aseguramiento exigido por el SP. Será el PEPS del país B quien haya realizado la traducción del nivel QAA solicitado al nivel de aseguramiento nacional. El PEPS podrá igualmente extraer información adicional de identidad del ciudadano que haya sido requerida por el SP (6) accediendo al Proveedor de Atributos (AP) necesario, si fuera posible.

Como puede observarse, y con el fin de reforzar un diseño centrado en el usuario, cualquier operación debe pasar por el usuario (redirecciones a través del navegador). Es más, en cada paso el PEPS implicado debe solicitar al usuario su consentimiento para realizar la acción estipulada. A pesar de ello, se ha intentando facilitar al máximo la interacción con el sistema, simplificando y homogeneizando la interfaz de usuario en todos los países.

Aunque la comunicación entre el usuario y el SP, y el usuario y el PEPS, se espera que sea vía HTTP, no deja de ser una decisión a nivel nacional, y queda fuera del ámbito del STORK. Sin embargo, STORK define SAML 2.0 como formato para el intercambio de la información de identidad del usuario, empleando el binding HTTP POST redirect para cumplir con el requisito de redirecciones a través del navegador del usuario. En este sentido, el PEPS del país A generará una solicitud de autenticación SAML (SAMLAuthnRequest) que será enviada al PEPS del país origen través del navegador del usuario. Tras el proceso de autenticación, el PEPS del país origen generará la respuesta que contenga la aserción sobre la verificación de la identidad del usuario (SAMLResponse). Esta respuesta se enviará al PEPS solicitante a través del navegador del usuario. En el último paso, el PEPS del país A enviará el resultado de la validación al SP, y, de nuevo, a través del navegador del usuario. De esta manera, el ciudadano ya está en disposición de acceder y realizar el trámite en el servicio del país de destino, al haber sido autenticado satisfactoriamente.

Los PEPS simplemente actúan como meros intermediarios en el proceso de autenticación. Por otra parte, las comunicaciones entre todos los actores se realizan mediante SSL/TLS. Por todo ello, la privacidad de los datos del usuario se protege durante todo el proceso de autenticación y acceso al servicio.

Por último, resaltar que en el contexto nacional español, la validación de las identidades electrónicas emitidas por los **Prestador de Servicios de Certificación** (PSC) nacionales, y basadas en certificados digitales, se realizará por medio de la Plataforma del Ministerio de Hacienda y Administraciones Públicas conocida como **@firma**. De esta forma, España permitirá a cualquier ciudadano que disponga de un certificado emitido por un PSC reconocido por el Ministerio de Industria, empezando por el DNIe electrónico, el acceso a servicios europeos de e-Administración de forma transparente a través de la Plataforma STORK. Además, como proveedor de atributos de identidad, que permita completar los datos de identidad del ciudadano que aparecen en los certificados y que son requeridos por el servicio al que quiere acceder el ciudadano para completar el proceso de autenticación o registro (por ejemplo, fecha o lugar de nacimiento, domicilio...), se integrará el servicio de Verificación de Datos de Identidad del Ministerio de Hacienda y Administraciones Públicas.

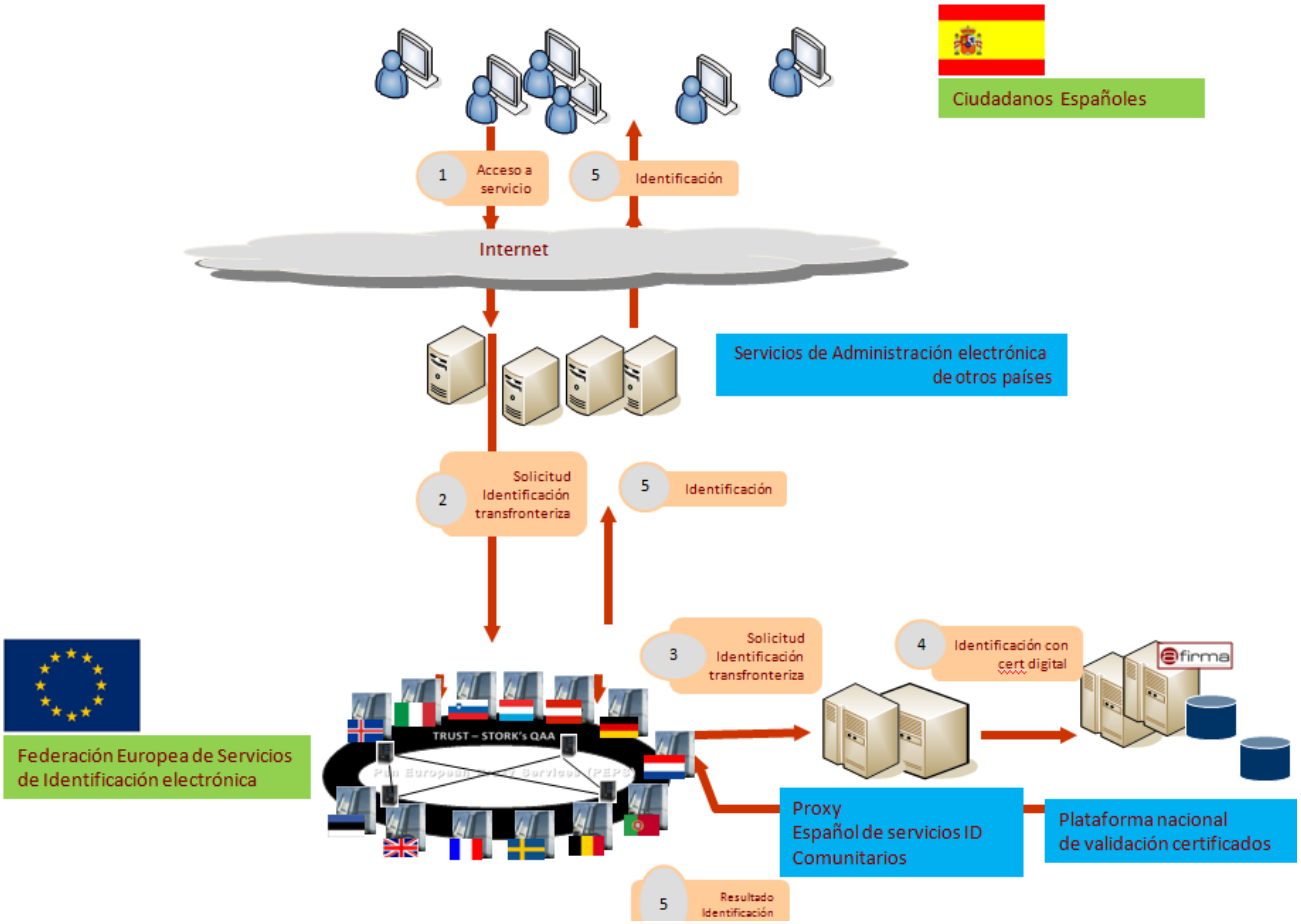


Figura 5. Integración de @firma al STOK

En la anterior figura, se presenta de manera esquemática, como se integrará @firma a la plataforma de intermediación del **STORK o federación europea de servicios de identificación electrónica, a través de su interconexión al PEPS nacional**. De esta manera se estará en disposición de identificar electrónicamente a ciudadanos españoles que quieren acceder a servicios de administración electrónica en otros estados miembros.

6 Conclusiones

Como conclusiones, podemos resaltar que Europa avanza en la tarea de definir y desarrollar la interoperabilidad de los identificadores electrónicos existentes en los estados miembros, de manera que se posibilite la movilidad plena de ciudadanos y empresas, y el consiguiente acceso a la administración electrónica en cualquier estado de manera transfronteriza y segura, al ser aceptados los eIDs foráneos europeos en cada país miembro.

Este proyecto, **posiblemente el mayor a nivel Europeo en materia de identidad electrónica**, pone a disposición de la AAPP europeas una plataforma de interoperabilidad que permitirá la identificación segura de los ciudadanos a través de sus identidades electrónicas de manera transparente y sencilla a través del intercambio de aserciones de identidad SAML, sin necesidad de que cada aplicación tengan que lidiar con la complejidad técnica de aceptar

diferentes tipos de identidades electrónicas de muchos países (múltiples tarjetas, drivers y certificados electrónicos).

La plataforma además de permitir identificar de manera segura a los ciudadanos, permite el intercambio de todos los datos de identidad y atributos que sean necesarios por parte de una aplicación, para completar un proceso de registro o autenticación.

Para España **supondrá la aceptación de los certificados digitales españoles, como los del DNI electrónico en servicios de Administración electrónica de otros países**, lo cual facilitará la relación de nuestros ciudadanos y empresas con otras AAPP europeas.

Todo ello se pone de manifiesto en los siguientes aspectos:

- El DNIe se está convirtiendo en un habilitador para el uso de técnicas de identificación segura y de firma electrónica por parte de los ciudadanos en nuestro país. Los servicios de la plataforma de validación y firma electrónica **@firma** como infraestructura común, es un catalizador para el desarrollo de servicios de administración electrónica seguros.

- La estrategia europea en materia de modernización tecnológica y mejora del acceso ciudadano a servicios públicos apuesta por nuevas soluciones y servicios que favorezcan el reconocimiento mutuo de las identidades electrónicas desplegadas en Europa. En esta línea, el proyecto STORK se erige como una apuesta pionera que implica a los principales gobiernos y representantes de la industria y centros de investigación europeos, y cuyo objetivo principal es el establecimiento de una Plataforma tecnológica de interoperabilidad de identidades electrónicas que permitirá a los ciudadanos establecer nuevas e-relaciones en Europa.

- Siendo conscientes de la legislación actual en materia de protección de datos, y con el fin de asegurar el éxito del proyecto en su fase de explotación, la arquitectura de STORK se ha diseñado para proteger la privacidad del usuario y posicionarle como principal actor en la transferencia de datos de identidad de los ciudadanos.

7 Acrónimos utilizados:

- **AP:** Proveedor de atributos de identidad
- **CIP**: Programa de Competitividad e Innovación de la Comisión Europea
- **eID**: Electronic Identity
- **IDABC**: Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (ver más en http://ec.europa.eu/idabc/)
- **IDP**: Proveedor Servicios de Identificación
- **PEPS**: Pan European Proxy Service
- **PKI**: Infraestructura de clave pública
- **QAA**: Quality Authentication Assurance
- **SAML**: Security Assertion Markup Language
- **SP:** Servicio de administration electrónica
- **STORK: S**ecure iden**T**ity acr**O**ss bo**R**ders linKed (nombre del Consorcio de 14 países para realizar pruebas en eIDM apoyadas por el CIP)

Más información sobre el proyecto en: https://www.eid-stork.eu/ y http://administracionelectronica.gob.es/es/ctt/stork