STORK: The European Electronic Identity Interoperability Platform

J. L. Hernández-Ardieta, *Member, IEEE*, J. Heppe and J. F. Carvajal-Vion

***Abstract*— The STORK project aims to achieve the interoperability of the European electronic identifiers, which will allow European citizens to establish new e-relations with the Public Administration and private sectors. These new e-relations will be tested by means of pan-European pilots, with new service providers being connected to the platform on a regular basis. As a result, in a medium term, every citizen will be able to establish a company, pay her taxes, or change her address without physical presence, and just by using her national eID independently of wherever the service is provided at. All European countries have already deployed electronic identity solutions. However, the level of assurance respecting each solution differs. Consequently, STORK has established a mapping between the levels of assurance of each country and a commonly agreed set of quality authentication assurance levels (QAA). Thanks to STORK design, service providers can interact with foreign users in a seamlessly and transparent fashion, delegating to STORK the particularities of each eID solution processing, while at the same retain the control respecting the required level of assurance in the user's identity. In any case, the user will always be able to control the data flow, aborting a transaction if desired. Explicit consent of the owner of the data, the user, is always required before sending her data from one entity to another. On the other hand, the platform does not store any personal data, so the user's privacy is guaranteed and enforced by design.**

***Keywords*— Electronic Identity, Authentication, Interoperability, Privacy.**

I. Introducción

La INICIATIVA "i2010 – La Sociedad de la Información y los Medios de Comunicación al Servicio del Crecimiento y el Empleo" [1] fue lanzada 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 el e-gobierno 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.

Un punto estratégico del Plan de Acción de e-Gobierno es el despliegue de soluciones de identidad o identificación electrónica (eID) en los Estados Miembro. Numerosos países ya disponen de infraestructuras para la emisión de identidades electrónicas (p. ej. España, Estonia, Italia, etc.), o están en pleno proceso de implantación de la nueva versión (Alemania).

Sin embargo, y con el fin de cumplir los propósitos marcados por la iniciativa i2010, es absolutamente necesario, que las identidades electrónicas nacionales sean reconocidas por los Estados Miembro ajenos al país emisor. De esta forma se fomentaría la movilidad de ciudadanos (estudiantes, trabajadores) europeos, el acceso a servicios gubernamentales y trámites administrativos y, en definitiva, el desarrollo de la economía europea al facilitar la implantación y consumo de nuevos servicios y ampliar los usuarios potenciales.

El objetivo del proyecto STORK (*Secure idenTity acrOss boRders linKed*) [2] 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 sus trámites y gestiones con las Administraciones Públicas de cualquier Estado Miembro 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. El Ministerio de la Presidencia español lidera el paquete de trabajo donde se define e implementa la plataforma de interoperabilidad. INDRA participa en el consorcio como empresa contratada por el Ministerio. 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.

Tras finalizar la fase de implementación, se va a proceder a desplegar e integrar una serie de pilotos que permitirán probar en un entorno real las capacidades de la plataforma de interoperabilidad desarrollada. Los pilotos estarán accesibles hasta Mayo de 2011, fecha de finalización del proyecto, 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.

Este proyecto está parcialmente subvencionado por la Comisión Europea dentro del programa ICT-PSP/2007/1 (ICT Policy Support Programme), englobado en el marco CIP (Competitiveness and Innovation Programme). INDRA participa como empresa contratada por el Ministerio de la Presidencia, miembro del Consorcio STORK.

J. L. Hernández-Ardieta, J. Heppe and J. F. Carvajal-Vion, Security Division, INDRA Sistemas, Madrid, Spain, jlhardieta@indra.es; jheppe@indra.es; jfcarvajal@indra.es.

J. L. Hernández-Ardieta is also Part Time Professor at the University Carlos III de Madrid.

- *SaferChat*, el cual desarrolla un entorno de mensajería instantánea seguro accesible a los usuarios mediante la autenticación con su identidad electrónica.
- *Student mobility*, 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.
- *Electronic delivery*, piloto que permitirá implantar un servicio de entrega electrónica basada en las infraestructuras nacionales.
- *Change of address*, el cual se centrará en un servicio de cambio de domicilio accesible mediante la identidad electrónica del país origen.

El resto del artículo describe en la sección II la arquitectura global de la solución, prestando especial atención al diseño centrado en el usuario y aseguramiento de la privacidad. Mencionar que la Plataforma STORK también ofrecerá un servicio de validación de certificados mediante el protocolo OCSP [3], que, por cuestión de espacio, no se describe en el artículo. Por último, se concluye el artículo en la sección III.

II. SERVICIO DE AUTENTICACIÓN PAN-EUROPEO

Esta sección detalla la arquitectura global del servicio de autenticación de la Plataforma. Cabe mencionar que uno de los mayores retos del proyecto ha sido diseñar una solución que integrara todas las particularidades y condicionantes legales nacionales en una única plataforma de carácter distribuido. En el proyecto se ha realizado un análisis profundo de la legislación europea aplicable y las transposiciones nacionales, destacando:

- Iniciativa i2010 [1], a la cual ya se ha hecho mención en la introducción.
- Directiva Europea de Firma Electrónica (1999/93/EC) [4].
- Directiva Europea de Protección de Datos [5], y la Directiva Europea sobre Privacidad y Comunicaciones Electrónicas (2002/58/EC) [6].
- Directiva Europea [7] de servicios en el mercado interno.
- Ley Española de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP) [8].

A. Marco para la interoperabilidad de las soluciones eID

Dado que existen soluciones de identidad electrónica (eID) más robustas que otras, el nivel de confianza o garantía respecto a la identidad del sujeto varía dependiendo de los aspectos técnicos y organizativos de la solución empleada. Por ejemplo, el soporte que almacena un par de claves criptográficas aporta mayores garantías si es un soporte hardware. Igualmente, el procedimiento seguido por la Autoridad de Certificación que emite el certificado correspondiente para identificar y registrar al usuario también puede fortalecer o disminuir este nivel. Un registro con verificación de identidad presencial aporta mayor confianza en el vínculo entre la identidad y la clave pública que una solicitud online.

Actualmente existe gran diversidad de soluciones 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 de interoperabilidad entre las diferentes soluciones existentes, denominado STORK QAA (*Quality Authentication Assurance*). Este modelo define cuatro niveles QAA para las soluciones eID. A mayor nivel, mayores garantías respecto a la identidad debe proporcionar la solución eID, y por tanto mayores requisitos deben cumplirse. 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 [9], y compatibles con los definidos en el marco de trabajo de garantía de identidad de Liberty [10].

Por otra parte, cada país define, de acuerdo a su marco legislativo y criterio nacional, los niveles de garantía de las soluciones eID que operan en sus fronteras. Por ello el modelo STORK QAA asocia los niveles nacionales de cada país a los niveles STORK QAA, de forma que se puede realizar una traducción de un nivel nacional a otro dentro de un marco de interoperabilidad común.

B. Arquitectura

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 gestión de las credenciales necesarias. Un proveedor 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 proveedores de servicio. Esta entidad también se encarga de validar la identidad cuando un proveedor de servicio o una tercera parte así lo requieren.

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 proveedor de servicio 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 proveedor de identidad del país origen que emitió la identidad al usuario.

Para permitir el diálogo entre los diferentes Estados Miembro (MS), se ha desplegado en cada país una entidad denominada PEPS (*Pan-European Proxy Service*) que integra las funcionalidades específicas de STORK. La siguiente Fig. 1 muestra la arquitectura distribuida diseñada.

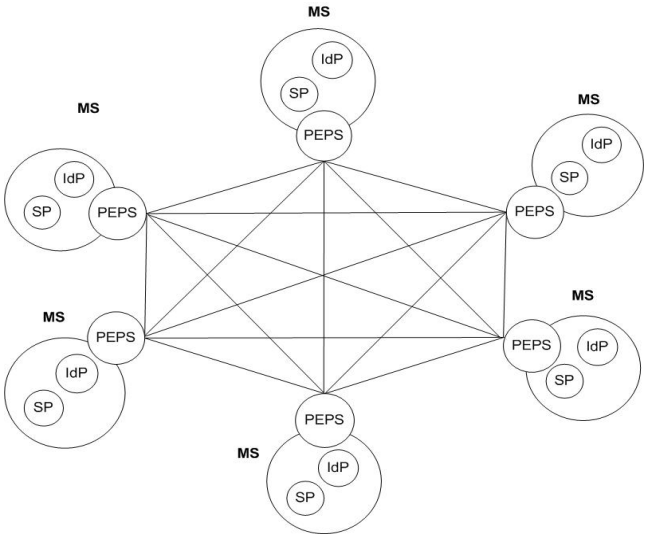

Figura 1. Arquitectura distribuída en malla desplegada

Como puede observarse en la Fig. 1 anterior, las comunicaciones se producen entre todos los PEPS, generando una arquitectura distribuida en malla. Cada PEPS dispone de una parte común a todos los países participantes, y de una parte específica que ha desarrollado cada país y que implementa sus singularidades concretas, como por ejemplo las interacciones con sus proveedores de servicio SP y proveedores de identidad IdP.

La siguiente Fig. 2 muestra de forma más detallada la comunicación que se produce entre todas las entidades implicadas.

Un usuario desea acceder a un servicio ofrecido por cierto proveedor en el país A (paso 1), y dispone de una solución eID emitida por un proveedor de identidad del país B (paso 0), del cual es originario. El proveedor del servicio obliga al usuario a autenticarse, siendo el mismo proveedor quien decide qué nivel de acceso se requiere. Dicho nivel estará en consonancia con los niveles nacionales, y será el PEPS del país A el encargado de asociarlo al nivel QAA correspondiente, tal y como se ha indicado en la sección II-A.

El proveedor del servicio redirigirá al usuario al PEPS del país A con el fin de gestionar su autenticación (pasos 2 y 3). El PEPS detectará el país de origen del usuario, remitiéndolo al PEPS correspondiente (paso 4). El PEPS del país origen redirigirá a su vez al usuario para que se autentique contra el proveedor de identidad que emitió su identidad electrónica (paso 5). En el ejemplo asumimos que dicha identidad cumple con el nivel de garantía exigido por el proveedor del servicio. Será el PEPS del país B quien haya realizado la traducción del nivel QAA solicitado al nivel de garantía nacional. El PEPS podrá igualmente extraer información adicional que haya sido requerida por el proveedor del servicio, accediendo al proveedor de atributos necesario (paso 6), 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 mediante 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 conseguir la máxima usabilidad posible, simplificando y homogeneizando la interfaz de usuario en todos los países.

Aunque la comunicación entre el usuario y el proveedor del servicio, y el usuario y el PEPS, se espera que sea vía HTTP,

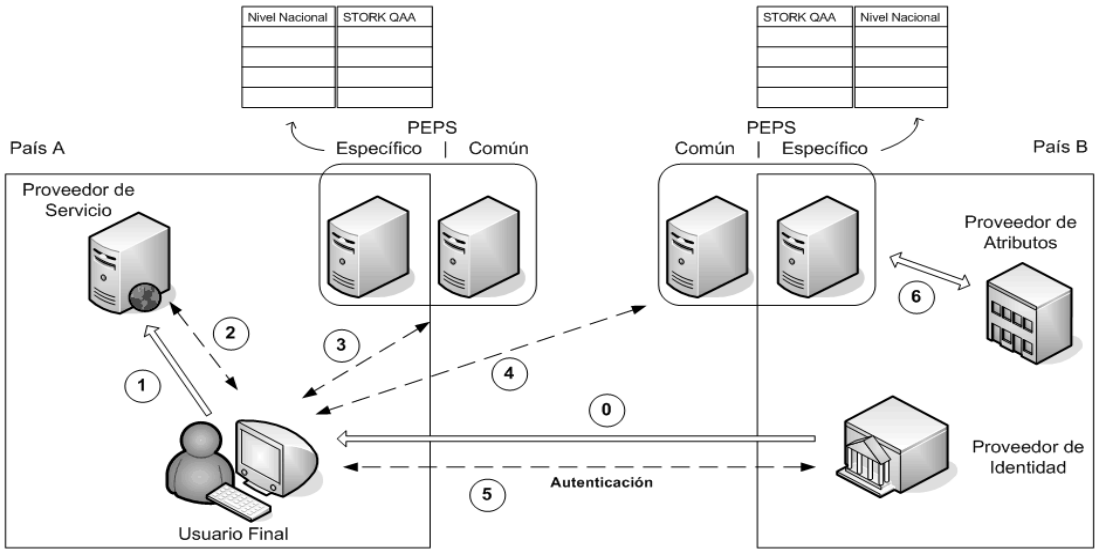

Figura 2. Arquitectura detallada para el servicio de autenticación

no deja de ser una decisión a nivel nacional, y queda fuera del ámbito del STORK.

Sin embargo, STORK emplea SAML 2.0 [11] como formato para el intercambio de la información de identidad del usuario, empleando la especificación (*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 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. 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 proveedor del servicio, y, de nuevo, a través del navegador del usuario.

Los PEPS simplemente actúan como meros intermediarios y traductores en el proceso de autenticación, no registrando ningún dato concerniente a los usuarios. Por otra parte, las comunicaciones entre todos los actores se realizan mediante comunicaciones seguras basadas en 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 Prestadores de Servicios de Certificación nacionales, y basadas en certificados digitales, se realiza por medio de la Plataforma del Ministerio de la Presidencia conocida como @firma [12]. De esta forma, España permitirá a cualquier ciudadano que disponga de un certificado emitido por un prestador de servicio de certificación reconocido el acceso a servicios europeos de e-Administración de forma transparente a través de la Plataforma STORK.

III. Conclusiones

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 información

Referencias

[1] *i2010 - Una sociedad de la información europea para el crecimiento y el empleo*, comunicación de la Comisión, de 1 de junio de 2005, al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones.

[2] Proyecto STORK. http://www.eid-stork.eu/

[3] *RFC 2560 – X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP*, Internet Engineering Task Force, Junio 1999.

[4] Directiva 1999/93/EC del Parlamento Europeo y del Consejo de 13 de Diciembre de 1999, por la que se establece un Marco Comunitario para la firma electrónica.

[5] 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.

[6] Directiva 2002/58/EC del parlamento europeo y del consejo de 12 de julio de 2002 sobre el procesamiento de datos personales y la protección de la privacidad en el sector de las comunicaciones electrónicas.

[7] Directiva 2006/123/EC del parlamento europeo y del consejo de 12 de Diciembre de 2006 servicios en el mercado interno.

[8] Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

[9] *Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms*, IDABC – European e-Government Service, Diciembre 2007.

[10] *Liberty Identity Assurance Framework*, Liberty Alliance Project, November 2007

[11] *Secure Assertion Markup Language (SAML) 2.0*, OASIS Standard, Marzo de 2005.

[12] @firma: Plataforma de Validación y Firma Electrónica. Ministerio de la Presidencia.

Jorge López Hernández-Ardieta (M'08) es Ingeniero Informático por la Universidad Autónoma de Madrid. Obtuvo el Diploma de Estudios Avanzados en la misma Universidad tras finalizar el primer ciclo de Doctorado en Ingeniería Informática y de Telecomunicaciones. Actualmente se encuentra finalizando su Tesis Doctoral en el Grupo de Seguridad de la Universidad Carlos III de Madrid. Ha trabajado como Ingeniero e Investigador en el área de Seguridad TIC desde el año 2002, participando en diversos proyectos de I+D+i tanto Nacionales como Europeos. Actualmente es Ingeniero Senior en la División de Seguridad de INDRA Sistemas S.A., y Profesor Asociado de la Universidad Carlos III de Madrid.

John Heppe, en sus 28 años de experiencia en el sector de tecnologías de la información, ha trabajado en varias compañías tanto en su país natal, Holanda, como en España. A lo largo de su carrera profesional se ha hecho un consultor experto en seguridad informática. Actualmente lidera, en representación del Ministerio de Presidencia, y junto con Bélgica, el paquete de trabajo que construye e implanta la plataforma de interoperabilidad de los identificadores electrónicos, como gran objetivo del proyecto STORK

José Fernando Carvajal Vión es Licenciado en Ciencias Biológicas por la Universidad Autónoma de Madrid. Tiene estudios de Doctorado en Ingeniería Informática por la Universidad Carlos III de Madrid. Es Máster en Gestión y dirección de la seguridad Por ASIMELEC-Universidad Pontificia de Salamanca. Master en gestión de proyectos de Innovación en el Hipersector eTIC por AETIC-LaSalle. Master en Técnico Superior de Prevención Riesgos Laborales especialidad seguridad. Está certificado CISA, CISM y CGEIT por la ISACA; y CISSP por ISC2. Cuenta con más de dieciocho años de experiencia profesional en el ámbito de las TIC, principalmente en el sector energético. Actualmente es gestor de proyectos de seguridad en el área de seguridad lógica de Indra Sistemas y es el principal responsable de los proyectos de R&D nacionales e internacionales del área de seguridad lógica. Pertenece a diferentes asociaciones y grupos de trabajo de seguridad y normalización de tanto nacionales como europeo.