Identity Services: electronic IDentification, Authentication and Signature (eIDAS)

Achieving the eIDAS vision through the Mobile, Social and Cloud triad[1]

Francisco Jordan · Helena Pujol· David Ruana
Safelayer Secure Communications S.A.

Resumen

El nuevo reglamento en identificación electrónica y servicios de confianza para transacciones electrónicas en el mercado interno pretende superar las barreras existentes en los servicios de identidad y firma electrónica. De acuerdo con el Jefe del Equipo de Legislación de la DG CONNECT de la Comisión Europea, la iniciativa eIDAS pretende: "Fortalecer el mercado único de la UE acrecentando la CONFIANZA y CONVENIENCIA en las transacciones electrónicas transfronterizas de forma segura y transparente".

A pesar de que la normativa propuesta es tecnológicamente neutral, creemos que la tecnología utilizada por la tríada Móvil, Social y Cloud puede estimular enormemente el despliegue de aplicaciones y, por lo tanto, puede acelerar la materialización de la visión eIDAS. Los dispositivos móviles se han convertido en el factor de autenticación hardware el "algo que se tiene" que habitualmente tenían los tokens. Los Smartphones permiten la implementación de mecanismos de alta seguridad y fáciles de usar que pueden complementar los eID nacionales ya existentes permitiendo mejorar la experiencia del usuario. Además, los servicios de identidad no son únicamente útiles para respaldar las identidades suministradas y gestionadas por los Estados Miembros, sino que también pueden mejorar los servicios proporcionados mediante la federación y la elevación de la confianza usando la identidad de las redes sociales o cualquier otro tipo de identidad usada habitualmente por los consumidores. Por último, los formatos y estándares Web centrados en el usuario y que tienen en cuenta la privacidad como OAuth y OpenID Connect facilitan a los desarrolladores el poder combinar identidades y funcionalidades que pueden revolucionar la cantidad y la calidad de las aplicaciones, en ambos casos debido a la plétora de dispositivos y a las ventajas proporcionadas por la computación en nube.

---

[1]Achieving the eIDAS vision through the Mobile, Social and Cloud triad". Versión publicada en "ISSE 2014 Securing Electronic Business Processes", ISBN: 978-3-658-06707-6, Editores: Helmut Reimer, Norbert Pohlmann, Wolfgang Schneider

1 Motivación

Desde antes de 1999, con la Directiva Europea de firma [EU99] se ha intentado establecer y regular un marco tecnológico y legal que permita, a los estados miembro de la UE en particular y de forma global en general, interaccionar de forma electrónica con seguridad y confianza. Hoy en día, una década y media después, honradamente, se puede afirmar que el objetivo perseguido en la línea de la Directiva no se ha cumplido. Los ciudadanos tienen un sistema de comunicación telefónica universal, un sistema de acceso a Internet universal, etc. pero no tienen un sistema de identificación, autenticación y firma electrónica universal.

Después de varios procesos de consulta, mucha actividad de grupos de trabajo y experiencia acumulada, en julio de 2014 es aprobado por el Parlamento Europeo el nuevo reglamento eIDAS [EU14] que actualiza la vieja Directiva de firma electrónica, y que entrará en vigor el 1 de julio de 2016, derogando automáticamente la antigua Directiva.

Por otro lado, fuera de Directivas, Reglamentos y otras actividades de regulación, observamos la realidad cotidiana de los ciudadanos y las empresas en la red, esto es, Internet. Sirva como ejemplo algunas de estas realidades irrefutables:

- En España el índice de penetración del teléfono móvil está sobre el 120%, y el de smartphones supera el 55% [Google13], siendo el mayor índice de Europa y subiendo anualmente en ratios mayores del 25%. No obstante, España ocupa el puesto 15 en penetración de smartphones, aunque está en la media de países desarrollados en cuanto penetración móvil (128%), y por encima de países en desarrollo que es del 89% [ITU14].
- Los datos de conexión a [ITU14] no son tan espectaculares, sobre todo en el mundo en desarrollo. Sobre el 30% de la población está conectada, comparado con más del 75% del mundo desarrollado. En hacer llegar Internet al máximo de la población mundial también tiene mucho que ver el móvil. Según [Cisco14], el tráfico móvil crecerá 3 veces más rápido que el fijo entre 2013 y 2018, y para 2018, el tráfico sin-hilos (wifi y móvil) superará al tráfico por hilos con 61% vs 39% del tráfico total respectivamente. No nos podemos olvidar de otros nuevos dispositivos de consumo como Tablets, SmartTVs, Games consoles, etc. que generan tráfico de datos,con una tendencia de convergencia de la información independiente de los dispositivos que posea el usuario.
- Cuando se habla de redes sociales basta con hablar de los números de Facebook[FB14]. Aproximadamente a principios de 2014, Facebook tenía1.300 millones de usuarios dados de alta, de los que se habla entre 680 y 1.000 millones lo son de smartphone. Y junto a esto, destacar también que existen 7 millones de aplicaciones y webs integradas con Facebook. A estos números hay que añadir el resto de redes sociales y grandes proveedores de servicios: Google+, Amazon, Yahoo, Microsoft, Salesforce, Twitter, LinkedIn, etc.
- En cuanto al Cloud (IaaS, PaaS, SaaS, MaaS, etc.) existen muchas predicciones de analistas y organizaciones sectoriales (Gartner, IDC, Cloud/Security Alliance, etc.) que sólo hablan de crecimiento y una tendencia imparable a la comoditación de la computación y el software como servicio. Este crecimiento se ve reforzado por beneficios muy claros, como ahorro de costes para las empresas y usuarios consumidores, y también para las empresas fabricantes y proveedoras de servicios, que al ahorro de coste y elasticidad en el crecimiento, hay que añadir el alcance global que ofrecen estas infraestructuras. A estas premisas hay que sumar de nuevo el avance imparable de los dispositivos móviles y, el acceso a Internet y servicios desde este medio. Se prevé que pronto el de-

sarrollo de Apps para móvil superará el de aplicaciones en PC/Desktop, lo que favorece de forma extrema el despliegue de servidores asociados en el Cloud.

Siendo claros, los grandes números que reflejan la realidad Social, Mobile y Cloud (conocida como SoMoClo o la tríada de la computación moderna) sobrepasan en órdenes de magnitud en cualquier aspecto (usuarios, aplicaciones, volumen de negocio, interés empresarial, tecnológico, etc) los números alrededor de la regulación de la firma electrónica y ahora su extensión también a la identidad electrónica. Se puede argumentar que se comparan cosas diferentes, pero en realidad, en este nuevo mundo globalizado, los grandes números son el principal indicador de las fuerzas que lo influencian y lo mueven.

Paradójicamente, **la seguridad y confianza** en general, y **la gestión de la identidad** en particular son temas principales y vitales para que la nueva sociedad digital se desarrolle plenamente. Así, estos se desarrollan y avanzan en armonía con las necesidades reales del momento, y lo hacen a velocidad Internet. Una regulación ayuda, pero sin la complicidad e involucración de los agentes a los que se regula, nunca alcanzará el éxito en su adopción. Probablemente, esta es la principal causa del poco éxito de la Directiva de firma electrónica 1999/93/EC, y esta debe ser la máxima a perseguir con el nuevo reglamento eIDAS.

En este artículo pretendemos transmitir cómo las fuerzas de Internet personalizadas en la tríada SoMoClo pueden servir para desarrollar de forma efectiva un nuevo reglamento basado en la identificación electrónica que mejore y aporte valor al statu-quo general.

2 Servicios de identidad (eIDAS)

Una constante en la evolución de las redes telemáticas, los servicios electrónicos e Internet en particular ha sido la gestión de la identidad. Los agentes participantes deben identificarse y autenticarse de forma electrónica. Todo empezó con una forma muy simple de identificación y autenticación mediante un nombre y un password ("factor algo que se sabe"). Décadas después, la realidad es que esta forma de identidad sigue siendo la más usada y presente en la red, independientemente de sus carencias conocidas y noticias frecuentes de "the password is dead".

Otra forma de identificación electrónica es la tarjeta inteligente PKI, como los citizeneIDs y ePassports, posiblemente, en el otro extremo de la cadena de uso y seguridad comparado con el usuario y password, mucho más seguro pero muchísimo menos usado. En este punto se debe decir que la Directiva de firma electrónica 1999/93/EC claramente apuntabaa la tecnología PKI en general, y la tarjeta inteligente PKI en particular como referencia de cumplimiento.

Entre ambos extremos, usuario y password (mínimo), y tarjeta inteligente PKI (máximo), siempre han existido puntos intermedios, y estos se ven ahora reflejados en el nuevo reglamento eIDAS, que al igual que ya propusiera la administración británica inicialmente [UKAuth00]y después popularizara el NIST de USA en la recomendación 800-63 [NIST06], ya no se habla de mecanismos concretos sino de niveles de garantía (LoA) de la identidad genéricos que clasifican los mecanismos en 4 niveles: bajo, medio, alto o muy alto.

El nuevo reglamento eIDAS[EU14] pone el acento en la eID de "electronic IDentification" a partir del cual se construyen los "trust services", de ahí también **Identity Services**. Por otra parte, los elementos básicos a partir de los que se desarrollan todos los servicios de confianza son "electronic Authentication" y "electronic Signature", de ahí que puestos juntos "**e**lectronic **ID**entification, **A**uthentication and **S**ignature" conformen las siglas de **eIDAS**. Es por esto que en la práctica y a lo largo del artículo manejemos de forma indistinta: **1)** *electronic identification and trust services*, **2)** *electronic IDentification, Authentication and Signature (eIDAS)*, o **3)** *Identity Services*.

Por completitud, aunque no se vayan a tratar de forma específica en este artículo, mencionamos también otros electronic trust services descritos en el reglamento eIDAS y construidos a partir de los básicos anteriores: 1) Electronic seals, 2) Time stamping, 3) Electronic registered delivery service, y 4) Web site authentication.

El reglamento eIDAS es neutral en cuanto a la tecnología.A lo largo de la historia han aparecido diferentes propuestas tecnológicas de las cuales algunas perviven y otras desaparecieron, a saber: Unix, Kerberos, X.509, Directory, LDAP,SSL/TLS, SAML 1.x, Liberty, SAML 2.0, OpenID, PKCS#, S/MIME, XML-DSig, CAdES, XAdES, PAdES, WS-*, etc. En este artículo nos interesa tratar las tecnologías alrededor de la tríada SoMoClo y, cómo estas pueden traspasar su caso de éxito a la implementación de la visión eIDAS.

3 La tríada“Social, Mobile and Cloud”

Es indiscutible la influencia de estos 3 vectores de la computación en los sistemas de información, la tecnología y la sociedad en general. Se puede hablar de una nueva era, una transformación a todos los niveles. Desde su caso de éxito, y dentro del alcance de su desarrollo, examinamos cómo se han resuelto los temas principales que nos ocupan en cuanto la “electronic identification, authentication and signature (eIDAS)”, y cómo podemos trasladarlos y/o mejorarlos de una forma genérica en una propuesta marco que ayude en la creaciónde una Internet más segura y de confianza en general, y sobre todo, más conveniente para los usuarios.

3.1 Social

Con Facebook y Google a la cabeza, las redes sociales y grandes proveedores de servicios en Internet son realmente los mayores proveedores de identidad (Identity Provider - IdP) que jamás han existido. No existe nada comparable en la historia de la gestión de la identidad y acceso (Identity and Access Management - IAM) a la capacidad de servicio de estos IdPs Sociales. Sólo con Facebook, 1300 millones de usuarios registrados pueden colaborar entre ellos practicando inicio de sesión único (Single Sign-On - SSO) a través de millones de aplicaciones terceras integradas. Aún más, un usuario puede tener varios eIDs Sociales (Facebook, Google, Twitter, …), y mediante técnicas de Federación de la Identidad pueden alcanzar todavía un mayor número de usuarios y aplicaciones hasta conseguir un acceso ubicuo a cualquier contenido, desde cualquier lugar, cualquier dispositivo y en cualquier momento.

Como es sabido, los IdPs Sociales despliegan mayoritariamente una identidad basada en una credencial de tipo usuario y password (“factor algo que se sabe”), la cual de forma opcional, puede complementarse con sistemas de password de un solo uso (One Time Password - OTP) a través de mensajes de texto SMS a un teléfono móvil (“factor algo que se tiene”). Por otra parte, como IdPs, las redes sociales implementan un paradigma centrado en el usuario (user-centric) que permite a estos gestionar todo tipo de atributos e información de identidad que pueden compartir de forma controlada con las aplicaciones y servicios que acceden, ayudando así a preservar su privacidad.

¿Qué hace posible que tantos centenares de millones de usuarios, millones de aplicaciones y servicios estén conectados y cooperen? No existe un motivo único, pero de entre todos, queremos destacar los que para nosotros son los necesarios: i) la **World Wide Web**, ii) el **paradigma user-centric**, y iii) la existencia de un nuevo modelo de economía de escala y creación de valor sin parangón conocido como la **API Economy**.

3.2 Móvil

El dispositivo móvil se está convirtiendo en el enlace directo de las personas con la sociedad digital. No es de extrañar entonces que todas las previsiones arrojen que el tráfico sin hilos (wireless en wifis y móviles) y que el ritmo de creación de aplicaciones para estos entornos superen a las clásicos del mundo con hilos.

Desde el punto de vista de la identidad y del exclusivo control del usuario sobre ésta, el dispositivo móvil es la herramienta perfecta. Hasta el momento, no existe ningún otro dispositivo electrónico más apegado al usuario, tanto desde el punto de vista de servicio como de preocupación en cuanto a su seguridad y privacidad. Con estas premisas, el dispositivo móvil se convierte también en un factor de seguridad importante para las transacciones electrónicas pudiendo aportar físicamente al usuario factores "algo que se tiene" y "algo que se es", éste último cada vez más presente con los sistemas biométricos de huella dactilar, reconocimiento de imagen y voz integrados en el dispositivo móvil.

Con estas premisas, es evidente que el dispositivo móvil puede aportar mucho en el terreno de la electronic identification, authentication and signature (eIDAS), incluso convertirse en el eID por excelencia del usuario de la sociedad digital. En esta línea, los servicios de confianza alrededor del móvil los denominamos de forma genérica **Mobile Identity Services**.

3.3 Cloud

La adopción de las tecnologías Cloud se considera imparable. Parece que los despliegues híbridos son los más aceptados, no sólo en una etapa de transición al Cloud, sino de forma permanente. Las organizaciones tienen sistemas e información más sensibles que no quieren externalizar y gestionar en el Cloud. Dentro de esta categoría entrarían los datos e información de identidad corporativos.

Las organizaciones demandan compatibilizar los sistemas existentes on-premise con nuevas aplicaciones y servicios en el Cloud, a la vez que gestionar de forma unificada las identidades de su población de usuarios. En este sentido cada vez es más normal ver como las organizaciones adquieren nueva computación y software como servicio para sus usuarios corporativos, a los que ofrecen de forma unificada, tanto los recursos on-premises y como los externos en el Cloud, compatibilizando el control de acceso y el inicio de sesión único (SSO) corporativo.

Esta realidad es asumida por los proveedores Cloud ofreciendo a las corporaciones sus servicios mediante integración a través de Federación de Identidades. De esta forma, los repositorios de identidad permanecen en las instalaciones de la organización y los usuarios corporativos se autentican siempre internamente, federando su identidad con el proveedor Cloud, que recibe la información mínima necesaria de identidad para suministrar sus servicios.

Como proveedor en el Cloud también podemos encontrar servicios de gestión de la identidad, o IDaaS (Identity as a Service). Estos proveedores ofrecen funcionalidad de gestión de la identidad en el Cloud tanto a corporaciones como a usuarios finales. En esencia, si hablamos de identidad basada en PKI, estaríamos hablando de una versión moderna y evolucionada de los Prestadores de Servicios de Certificación (PSCs).

4 La implementación

Asumido que los vectores Social, Mobile and Cloud pueden ayudar a desplegar y acelerar el éxito de la nueva propuesta de reglamento eIDAS, y examinados los aspectos de estos relacionados con la gestión de la identidad, a continuación proponemos un solución tecnológica que implementa el sistema que, desde nuestro punto de vista, puede tener en estos momentos

mayor probabilidad de éxito para cubrir los objetivos eIDAS a nivel Europeo en particular, y Global en general, en cuanto a la electronic Identification, Authentication, and Signature.

Proponemos un framework distribuido que queda definido por su: i) Arquitectura, ii) Protocolos y iii) Servicios. Este framework tecnológico establece los servicios básicos de confianza a partir de los cuales se pueden construir otros servicios de confianza más avanzados. Por otra parte, en la medida de lo posible, el sistema propuesto se basará en servicios, protocolos y arquitecturas ya existentes que han demostrado un uso y despliegue masivo, como las presentes en Internet y los escenarios Social, Mobile and Cloud.

4.1 Arquitectura

La arquitectura del framework tecnológico eIDAS propuesto puede resumirse gráficamente en el siguiente esquema.

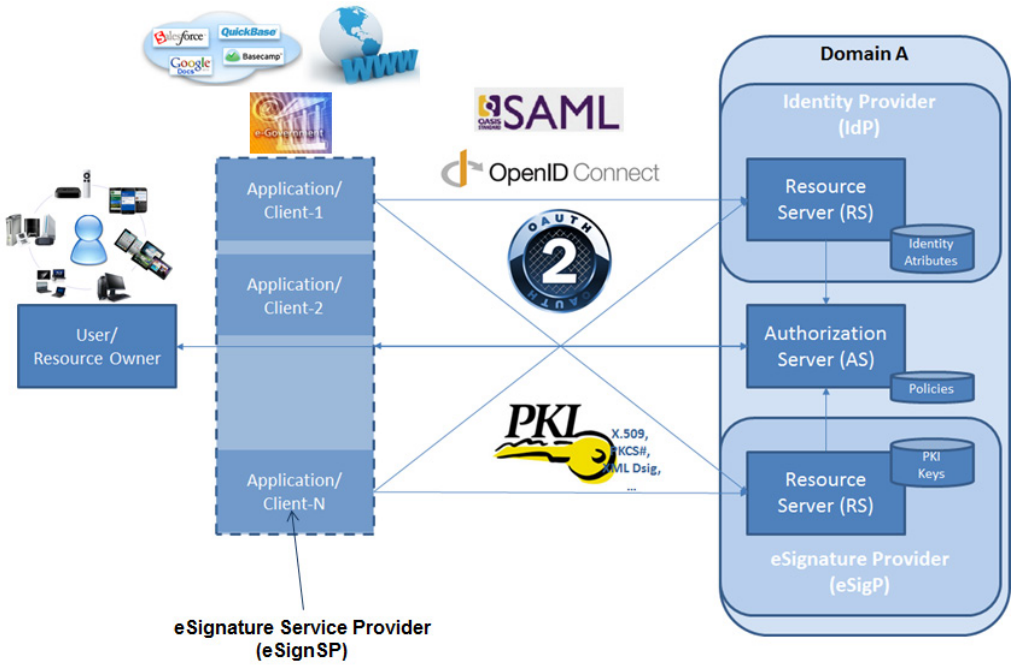

Fig. 1: Arquitectura básica Framework Tecnológico eIDAS

Siguiendo el esquema de éxito de grandes proveedores de servicios Internet (Google, Amazon, etc.) y redes sociales (Facebook, Twitter, etc.), el modelo arquitectónico de identidad implementa un paradigma user-centric en el que i) los usuarios pueden explícitamente consentir/autorizar la entrega de información de identidad a las aplicaciones que acceden, o ii) el sistema provisión de identidad (IdP) define políticas de autorización administrativas que el usuario conoce y consiente implícitamente.

El modelo obedece al framework de autorización OAuth 2.0 [OAuth12] con soporte OpenID-Connect 1.0 [Connect14] y SAML 2.0 Web SSO Profile [SAML05] para la autenticación. Estos protocolos descansan sobre una infraestructura pura Web siguiendo un paradigma RESTful, y hoy en día, constituyen la base técnica de los sistemas que soportan centenares de millones de usuarios que realizan billones de interacciones e invocaciones de servicio en la red. De hecho, son el framework que hacen posible el éxito la tríada de computación Social, Mobile and Cloud.

La arquitectura es una fusión del modelo 3-legged clásico ya practicado en SAML –User, ServiceProvider (SP), IdentityProvider (IdP)- con el modelo 3-legged de OAuth y la presencia de las entidades User, Relying Party (RP) y Authorization Server (AS). El resultado es la combinación de un IdP con un AS, siendo las entidades SP y RP la misma entidad con diferente nombre, y el User el mismo en ambos casos. La ventaja del framework de autorización OAuth es que puede integrar cualquier mecanismo de autenticación, desde el simple usuario y password, pasando por credenciales eIDs de alta seguridad, hasta otros framework de autenticación como SAML.

4.1.1 Identity Provider (IdP)

Este componente del framework implementa la funcionalidad propia de un proveedor de identidad, esto es, gestión de atributos de identidad, autenticación, SSO y Federación. En este caso, además incorpora una funcionalidad adicional propia del modelo OAuth, un Resource Server (RS) que mapea conjuntos de atributos de identidad del usuario (Owner) en scopes OAuth, sobre los cuales, las Relying Parties (RPs) pueden solicitar autorización al usuario para su acceso a través del Authorization Server (AS). Como ya se ha mencionado, esta autorización o consentimiento puede ser explícito o implícito.

La incorporación de un RS/AS en el IdP para acceder a atributos de identidad ofrece un interfaz y un modelo claro de acceso que tiene en cuenta el control de los datos del usuario, y por tanto su privacidad. Este modelo ya ha demostrado sobradamente su utilidad en las redes sociales, no sólo por ofrecer la posibilidad al usuario de controlar a quién da sus datos, sino también, por estandarizar un interfaz de programación (API) que las aplicaciones pueden integrar fácilmente. Así, y sirva de ejemplo, parece natural trasladar el mismo modelo a las aplicaciones de la Administración Pública para disponer de un mecanismo de integración dónde, independientemente del eID que utilicen los ciudadanos para su autenticación, pueden obtener, opcionalmente bajo consentimiento explícito, acceso a datos de los usuarios.

4.1.2 eSignature Provider (eSigP)

Este componente del framework es en esencia un Resource Server (RS) especializado en atributos de identidad PKI, en concreto, claves y certificados PKI a utilizar en firma electrónica. Como en el caso anterior, el RS delega en el AS el proceso de autorización, que a su vez, delega en el IdP el proceso de autenticación. De esta forma, obtener autorización de acceso para un atributo PKI es equivalente a hacerlo para un atributo normal. No obstante, el acceso al atributo "clave privada PKI" no desemboca en el retorno del valor del atributo, sino en el uso de la "clave privada", esto es, en un proceso de firma electrónica básico, como por ejemplo en el caso de claves PKI RSA, generar un bloque PKCS#1 [PKCS03].

Una característica del RS de claves PKI es la de abstraer el repositorio físico donde se almacenan de forma segura las claves. Inicialmente, se contemplan dos modos de funcionamiento dependiendo del repositorio físico (ver Fig. 2):

- **server-signing**, las claves se almacenan en un Hardware Secure Module (HSM) conectado localmente al RS, en el que el control de la activación de las claves por el usuario se hace de forma indirecta a través del RS (sole-control level 1 [CEN13]), o directamente (sole-control level2), o
- **mobile-signing**, las claves se almacenan en un dispositivo del usuario, por ejemplo un móvil, bajo su control directo y exclusivo (sole-control level 2).

El modelo OAuth permite aplicar de forma estándar un proceso de consentimiento (autorización) para conseguir el acceso al recurso clave PKI del usuario para generar una firma-e, consiguiendo así de manera natural la conformidad explícita del usuario que firma.

4.1.3 Relying Parties y Aplicaciones

Siguiendo el modelo OAuth, una Relying Party (RP) es un componente cliente (Client) que accede a los recursos en un RS controlados por un AS en nombre de los usuarios. En nuestro framework, una vez autenticado un usuario y dado su consentimiento, explícito o implícito, las RPs podrán acceder a información de identidad compuesta por atributos de identidad normales y/o PKI. El acceso a clave privada PKI para realizar una firma-e básica.

Una aplicación a destacar es la de firma electrónica avanzada (AdES) en general (en el dibujo nombrada como eSignature Service Provider –eSignSP-), y en particular siguiendo un formato específico como por ejemplo PDF con PAdES. La aplicación soporta recibir un documento PDF y generar otro documento PDF que incorpora la firma-e PAdES de un usuario. Para ello la aplicación actúa como RP/Client del framework iniciando un proceso de autorización para obtener el consentimiento del usuario. Una vez autenticado el usuario, y dado su consentimiento, la aplicación puede ordenar la firma del PDF en nombre del usuario.

Como ya ocurre en Internet, se pueden crear aplicaciones complejas a partir de la composición y agregación de diferentes servicios. Por ejemplo, el usuario almacena sus documentos PDF en un servicio Cloud. La aplicación pide autorización al servicio Cloud para obtener un documento PDF, y a partir de este punto, la firma-e del documento transcurre como antes.

En este caso, se están accediendo servicios en dominios de identidad diferentes (almacenamiento Cloud y firma-e) agregados en una aplicación. Esto implica que el usuario será autenticado dos veces. No obstante, nuestro framework, a través del IdP, permite federar dominios de identidad externos y entonces aplicar SSO. No obstante, los dominios de identidad externos federados pueden tener un nivel de garantía (LoA) de la identidad menor del requerido para poder acceder al servicio de firma-e. En este caso, el framework realizará un step-up de autenticación (SSO Adaptativo) requiriendo al usuario un factor adicional que cumpla el requisito demandado, por ejemplo, un PIN estático memorizado o dinámico a través de SMS. De esta forma, se consigue la conveniencia de la federación y el cumplimiento de los requisitos de garantía de confianza.

4.2 Protocolos

Los protocolos en los que se basa el framework son estándares (de facto o de jure) bien conocidos y extendidos en Internet, y son los que soportan toda la actividad Social, Mobile y Cloud. Los protocolos principales son aquellos que forman parte intrínseca del framework y soportan los servicios y funcionalidades de los componentes IdP y eSigP.

En **autenticación** se proponen los protocolos OpenID Connect 1.0 y SAML 2.0, el primero porque se basa en OAuth y del segundo se debe soportar sólo el perfil Web Browser SSO que aporta una funcionalidad similar a OpenID Connect, y se usará para conectar y hacer SSO en sistemas empresariales que de momento no han adoptado OpenID. NOTA: Existe la opinión que SAML es un sistema de transición hasta que OpenID Connect sea desarrollado y asumido en su totalidad [MaBa12].

Estos protocolos permiten estandarizar los servicios y funcionalidades de representación e intercambio de atributos de identidad, autenticación, SSO y federación, que son las funciones propias de un Identity Provider (IdP). En cuanto a la normalización de nuevos mecanismos de autenticación como los biométricos, FIDO [FIDO14] es la opción preferente para la interoperabilidad de mecanismos de autenticación genéricos.

OAuth 2.0 para **autorización** (consentimiento) del usuario en el acceso por parte de aplicaciones a sus recursos. En nuestra opinión, el framework de autorización OAuth es realmente el responsable de la implementación de estas nuevas tecnologías y métodos que han hecho

posible el fenómeno Social, Mobile y Cloud en particular, y el nuevo impulso de avance de Internet en general. El éxito de OAuth ha sido estandarizar una forma sencilla de acceder a recursos totalmente compatible con la infraestructura Web de Internet (HTTP) utilizando métodos algo más sofisticados, pero sencillos y suficientes, e incorporar el respeto a la privacidad con un paradigma user-centric. De OAuth, se excluyó explícitamente la autenticación, ofreciendo así un sistema abierto en el que se puede integrar cualquier mecanismo.

OAuth y OpenID Connect como base de la implementación de un servicio básico de **firma electrónica** delegado en el que se representan y gestionan atributos PKI. En el caso de la clave pública a través de un tipo de atributo dentro del perfil del usuario (e.g. X.509), y en el caso de la clave privada a través de un servicio de firma-e en el que se aplica el algoritmo privado correspondiente (e.g., RSA para generar un bloque PKCS#1). En esta primera implementación se integran las infraestructuras PKI basadas en X.509, aunque el modelo es abierto a cualquier infraestructura.

Este modelo permite implementar de forma natural una arquitectura de sistema de confianza para firma-e basada en servidor tal y como se plantea en **TW4S** [CEN13]. Adicionalmente, y gracias a la abstracción de OAuth y su paradigma user-centric, el mismo esquema sirve para definir un sistema de confianza para firma-e basado en mobile como dispositivo de creación de firma –SCDev- alcanzando el nivel 2 de sole-control (ver Fig. 3). Nótese que el módulo conceptual **Trustworthy Signature Creation Module (TSCM)** tiene una gran similitud con los componentes eSigP y AS de nuestra arquitectura (ver Fig.2).

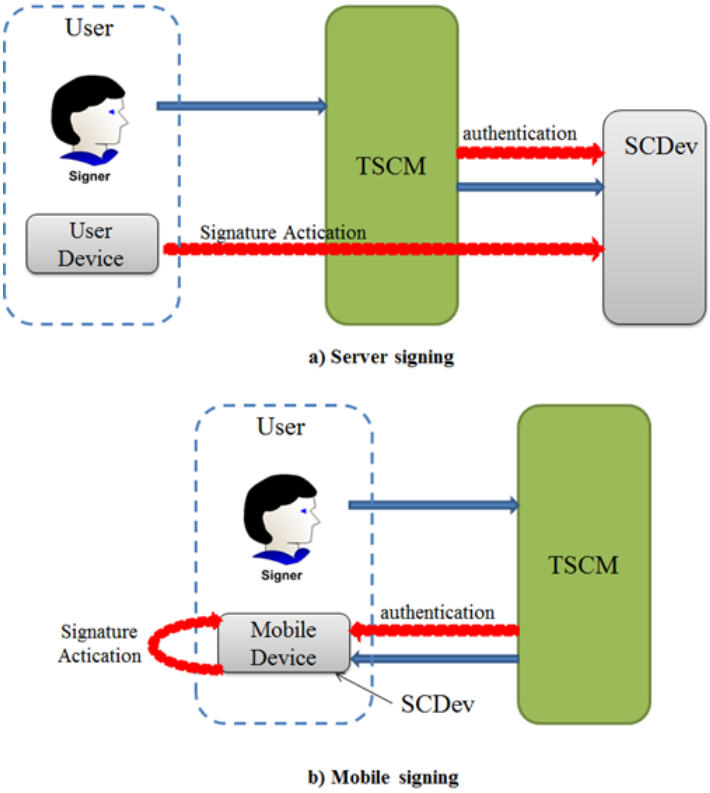

Fig. 2: Trustworthy Signature Creation Module (TSCM)withlevel 2 sole control

Por otra parte, es fácil comprobar que el framework planteado también sirve para implementar los escenarios de firma electrónica basados en mobile descritos en “Rationalised Framework of Standards for Advanced Electronic Signatures in Mobile Environment” [Pope13]. En este

framework se proponen escenarios basados en mobile y servidor de forma separada, al igual que escenarios mixtos mobile y servidor, en el que el dispositivo móvil sirve en realidad de autenticador para activar la firma-e en el servidor.

Adicionalmente a estos protocolos principales, el sistema debe soportar alguno(s) de los formatos de contenido y/o documentos con sus respectivos protocolos de firma electrónica estándares. Concretamente, de forma inicial aquellos que definan firmas electrónicas basadas en tecnología PKI sobre el estándar X.509. En particular:

- Formatos simples, como PKCS/CMS, XML-DSig, S/MIME, etc.
- Formatos avanzados, como los ETSI CAdES, XAdES y PAdES.

Con respecto a la arquitectura propuesta en este artículo, la implementación de los formatos de firma correspondería al componente eSignature Service Provider (eSignSP) que actuaría como RP/Client del servicio de firma-e básico eSigP.

4.3 Servicios

El framework debe proporcionar los siguientes **servicios y funcionalidades básicas** de confianza: Electronic Identification, Identity Assurance, Authentication, Authorization, Single Sign-On, Federación y Electronic Signature.

Los servicios de **Electronic Identification** permiten registrar, emitir y gestionar el ciclo de vida de eIDs de cualquier tipo, así como asociar a estos identificadores únicos un conjunto de atributos de identidad que definen al usuario en el ciberespacio. En general estos servicios están muy ligados al tipo de eID y de repositorio de identidad que se utilice. De especial interés son los eIDs basados en PKI, y en particular, los custodiados en Mobile y Servidor. Nuestro framework asume una provisión y gestión de eIDs externa, ya que nos interesa formalizar el uso de estos eIDs para potenciar la interoperabilidad e integración en aplicaciones.

Con la función de **Identity Assurance,** el framework debe permitir clasificar de una manera uniforme el nivel de garantía (LoA) que ofrece una identidad concreta, y así comparar de forma abstracta y relativa las garantías de confianza de cualquier eID. De base se usará la escala del NIST 800-63de 4 niveles (bajo, medio, alto y muy alto), y por extensión, cualquier otra escala basada en niveles que se mapeen a la del NIST, por ejemplo la del proyecto STORK o la del Esquema Nacional de Seguridad (ENS) en España.

Los servicios de **Authentication** permitirán corroborar la identidad electrónica a partir de credenciales eID de los participantes mediante la ejecución de un protocolo seguro que contribuirá en la determinación de garantía (LoA) de la identidad en práctica.

Dentro de autenticación, la funcionalidad de **Trust Elevation and Step-up** posibilitará establecer una serie de mecanismos que permiten elevar la confianza en un eID dentro de un nivel LoA, o que permiten saltar de nivel LoA complementando el eID inicial con otra credencial, así acumulando factores de autenticación. Estas funcionalidades tienen que ver con autenticación contextual, basada en el riesgo y adaptativa [OASIS14].

Los servicios de **Authorization**, desde un punto de vista de paradigma user-centric de la gestión de la identidad, el framework debe poder permitir al usuario consentir (autorizar) de forma explícita la entrega de atributos de identidad a un proveedor de servicio (SP) o Relying Party (RP) con la que interactúe. Esta funcionalidad dota al framework de un carácter respetable con la privacidad de los datos de identidad de los usuarios.

Los servicios de **Single Sign-On (SSO)** permiten a los usuarios y aplicaciones inicio de sesión único dentro de una federación de confianza, esto es, el usuario se autentica una vez y

accede a múltiples aplicaciones y servicios sin re-autenticar. Con **Adaptive SSO,** función relacionada con trust elevation y step-up, se permite practicar SSO a una aplicación o servicio siempre y cuando el usuario previamente autenticado disponga de un nivel LoA igual o superior al requerido en el nuevo acceso. En el caso contrario, se podrá re-autenticar al usuario para obtener un mayor nivel LoA, y así ganar el nuevo acceso en caso de éxito.

Los servicios de **Federation** permiten que los usuarios pueden enlazar (link) diferentes identidades y atributos de identidad que gestionan diferentes sistemas de identidad (IdPs) y así poder hacer SSO entre aplicaciones de sendos dominios o federaciones. Por ejemplo, un usuario puede federar una cuenta social con una cuenta corporativa para mejorar la experiencia de acceso a ciertos recursos de la corporación. No obstante, deberá practicarse SSO Adaptativo ya que sin duda habrá recursos de la empresa que requieran de un mayor nivel LoA.

En este caso, nos interesa formalizar la **Electronic Signature** como una función en la que se aplica una credencial para producir una firma electrónica avanzada en los términos definidos en la cláusula (11) del artículo 3 de la nueva regulación eIDAS. De estos requisitos se desprende que el sistema de firma electrónica está fuertemente integrado con el sistema de gestión de la identidad. Desde nuestro conocimiento y experiencia, la propuesta técnica presentada en este artículo es capaz de implementar estos requisitos.

Como ya se ha mencionado, existen otros tipos de servicios de confianza que en general se implementan sobre los servicios básicos antes descritos. No obstante, estos servicios avanzados no son objeto de este artículo.

5 Conclusión

Después de una década y media de la Directiva de firma electrónica 1999/93/EC, estamos ya en el proceso de cambio al nuevo reglamento eIDAS, esta vez sí, involucrando directamente la identificación y autenticación, partes esenciales del que se deriva un mejor framework de firma y otros servicios de confianza avanzados.

No obstante, se ha visto que la regulación no es suficiente para dinamizar y mejorar un mercado. Los ciudadanos, consumidores, organismos públicos, empresas, organizaciones y usuarios en general, deben encontrar valor en los servicios electrónicos que van a consumir, y además como en todo, la relación coste-beneficio para ellos debe estar claramente decantada hacia el beneficio. La inconveniencia del usuario es un coste muy alto, y la seguridad y confianza son un coste que debe maximizar el beneficio. Diseñar un servicio electrónico sin estas premisas claras va contra los principios económicos más básicos.

Proponer un marco de servicios electrónicos en la línea de los servicios en Internet que más usuarios y éxito tienen en la actualidad, y acompañarlo de un marco de seguridad y confianza adaptado a las necesidades del servicio en todo momento, parece una fórmula con mayor probabilidad de éxito. El identificador electrónico, la autenticación y la firma deben adaptarse al servicio de valor que se presta maximizando el par coste-beneficio. Para esto, deben convivir múltiples eIDS y mecanismos de autenticación que cubran todos los niveles de garantía (LoA), desde bajo hasta muy alto. Esto es lo que en Safelayer hemos llamado de forma genérica **seguridad y confianza adaptativa**.

Nuestra propuesta de framework técnico eIDAS está situada estratégicamente para explotar lo que algunos expertos han denominado la "**API Economy**", un nuevo y evolucionado tipo de modelo de negocio en el mundo actual de servicios en Internet, redes sociales y aplicaciones móviles, en el que los grandes proveedores de servicios, Cloud y redes sociales están perfectamente situados. En este nuevo modelo, el paradigma service-centric de gestión de la identi-

dad no escala, por eso protocolos como OAuth, OpenID Connect y SCIM [SCIM14] sobrepasarán antiguos protocolos como DSML, SAML y XACML [MaBa12].

En la API Economy, empresas, organizaciones y proveedores en general publican unos interfaces de programación (API) web que permitirán el acceso a recursos en general, y a recursos de identidad de sus usuarios en particular. Estas APIs podrán ser integradas y agregadas con otras APIs por proveedores que generaran nuevos servicios de valor alrededor de una comunidad de usuarios específica. Este fenómeno no sólo retendrá a los usuarios actuales sino que atraerá a nuevos usuarios que harán crecer la comunidad. El crecimiento de la comunidad, a su vez, atraerá a más proveedores de nuevo valor que aportará más usuarios. Y así, se producirá una espiral de creación de valor que crea una economía de escala sin precedentes.

En realidad, esta nueva economía digital ya ha llegado, es la nueva economía en la que se basa el éxito de Google, Facebook, Amazon, Salesforce, eBay, Netflix, etc. Los sectores más innovadores ya lo han entendido y están acercando el Cloud, las redes sociales y la movilidad a su negocio principal. Las administraciones públicas no serán ajenas a esta nueva economía y acabarán dando acceso a los ciudadanos a partir de un eID social, al mismo tiempo que, siguiendo una estrategia OpenData, ofrecerán a la industria acceder de forma controlada a información de identidad de los ciudadanos.

En definitiva, es en este marco técnico y de mercado donde el desarrollo de la nueva propuesta de regulación eIDAS debe encajar, y es en este marco dónde se sitúa nuestra propuesta de framework técnico de seguridad y confianza para la identificación electrónica, autenticación y firma.

References

[EU99] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.Official Journal L 013, 19/01/2000 P. 0012 – 0020

[EU14] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[Google13] "Our Mobile Planet: Spain. Understanding the Mobile Consumer", Google, May 2013, http://services.google.com/fh/files/misc/omp-2013-es-en.pdf, seen on July 10th 2014

[ITU14] "The world in 2014. ICT Facts and Figures", ICT Data and Statistics Division Telecommunication Development Bureau, ITU, April 2014

[Cisco14] "Cisco Visual Networking Index: Forecast and Methodology, 2013–2018", Cisco, June 2014

[FB14] Statistic Brain - Facebook Statistics, January 2014, http://www.statisticbrain.com/facebook-statistics/, seen on July 10th 2014

[Gartner13] E. Andersonet al., "Forecast Overview: Public Cloud Services, Worldwide, 2011-2016, 4Q12 Update", Gartner Inc., February 2013

[UKAuth00] "Authentication Framework v1.0", Office of the e-Envoy, December 2000

[NIST06] W.E. Burr, D. F. Dodson and W. T. Polk, "Electronic Authentication Guideline", Special Publication 800-63, Version 1.0.2, National Institute of Standards and Technology, April 2006

[OAuth12] D. Hardt, "The OAuth 2.0 Authorization Framework", RFC 6749, IETF, October 2012

[Connect14] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros, C. Mortimore, "OpenID Connect Core 1.0", February 2014

[SAML05] S. Cantor et al.,"Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS SSTC, March 2005

[PKCS03] J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography. Specifications Version 2.1", RFC 3447, IETF, February 2003

[CEN13] Draft for publication of CEN/TS 419241 Security Requirements for Trustworthy Systems Supporting Server Signing, European Committee for Standardization, December 2013

[MaBa12] Maler, Eve; Barton, Tom: The Future of Federated Identity or, Whither SAML?InCommon, July 2012

[FIDO14] The FIDO Alliance, https://fidoalliance.org, seen on July 10th 2010

[Pope13] N. Pope, J. C. Cruellas, I. Khan, J. Olnes, A. Tauber, "Rationalised Framework of Standards for Advanced Electronic Signatures in Mobile Environment", SR 019 020 (Draft), ETSI, December 2013

[OASIS14] OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation)

[SCIM14] K. Grizzle, P. Hunt, E. Wahlstroem, C. Mortimore, "System for Cross-Domain Identity Management: Core Schema", Internet Draft, IETF, June 2014