Universitat Oberta de Catalunya

uoc.edu

Cloud Docs Platform

Jose Luis Prieto Sancho
Máster universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones

Juan Carlos Fernandez Jara
Victor García Font

31 de diciembre de 2018

A copy of the license is included in the section entitled "GNU Free Documentation License".

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Cloud Docs Platform*
Nombre del autor:	*Jose Luis Prieto Sancho*
Nombre del consultor/a:	*Juan Carlos Fernández Jara*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	12/2018
Titulación:	*Máster universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)*
Área del Trabajo Final:	*Ad hoc*
Idioma del trabajo:	*Español*
Palabras clave	*Cloud Docs Signature*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

En vista a la evolución en la seguridad, movilidad y descentralización de servicios se promueve la elaboración de una plataforma que unifica estos términos. Todo ello con ayuda del nuevo marco eIDAS (Identificación Electrónica y los Servicios de Confianza) presentado en el reglamento (UE) Nº 910/2014 del Parlamento Europeo que define la interacción segura entre empresas y el reconocimiento de las condiciones en todos los estados.

Esta nueva plataforma también hace uso de los famosos servicio en la nube, como son Google Drive, Dropbox, Box, que permiten el almacenamiento de documentos de forma segura y remota.

Con todo ello conseguimos un servicio puente de autentificación de confianza y firma segura funcionando como SaaS.

Abstract (in English, 250 words or less):

As the evolution in security, mobility and decentralization of services becomes a platform to unify these terms. All this with the help of the new eIDAS framework (Electronic Identification and Trust Services) presented in Regulation (EU) No. 910/2014 of the European Parliament that defines the safe interaction between

companies and the recognition of conditions in all states.

This new platform also makes use of the famous service in the cloud, such as Google Drive, Dropbox, Box, which allow the storage of documents safely and remotely.

With all this we get a reliable authentication bridge service and secure signature working as SaaS.

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

En la actualidad cualquier tipo de servicio se está encaminando a una globalización, llegando a un nivel considerable en la cultura política, en ordenamiento jurídico y económico nacional, y en sus relaciones nacionales e internacionales [1].
El principal problema en el mundo de la seguridad digital, y el porqué de este proyecto, es que cada estado tenía su propio método de interpretación por lo que la autenticidad de la firma era complicada al intervenir varios estados.
Ese enfoque ha hecho que se recree un nuevo marco en la unión europea en base al campo de la seguridad donde se delimitan las acciones y procesos para tener en cuenta por cada uno de los estados miembros para definir un único reglamento que garantiza la aprobación de interacciones electrónicas entre empresas, más rápidas y seguras indiferentemente del estado.
Este reglamento definido con las siglas eIDAS (Identificación electrónica y servicios de confianza) proporciona las funciones elementales para realizar cualquier tipo de transacción online. Las cuales son extensibles en su totalidad en el ámbito de la ciudadanía y empresarial.
Gracias a este proceso la unión europea levanta una de las barreras comunicativas muy importantes como puede ser en el ámbito jurídico.
Se define así una solución flexible y segura con la que poder interactuar con diversos servicios.

Actualmente existen servicios para la firma y sellado electrónico que requieren de una plataforma hardware y la mediación de una instalación software que el usuario tiene que llevar a cabo antes de proceder con la firma de un documento. Mediante la utilización del reglamento eIDAS facilitamos la utilización en un modo más descentralizado, flexible y móvil, reduciendo la actuación de un usuario experto y facilitando su uso a unos pocos pasos. En resumen, se pretende se mas optimo, seguro y sencillo.

Un gran porcentaje de la población hace uso de herramientas de almacenamiento en la nube (cloud). Un término que en esta última década ha ido calando cada vez más en la idea de infraestructura de internet. Y siendo mencionado como un servicio importante en la vida personal y empresarial de cada individuo. Puesto que facilita el almacenamiento y transferencia de documentos sin tener un soporte físico. Utilizando estas herramientas de almacenamiento junto a eIDAS obtenemos un software minimalista de bajo consumo usado bajo demanda en una plataforma web, más claramente expuesto como concepto de SaaS (Software como Servicio).

Para resolver los problemas anteriormente mencionado y por el cual se lleva a cabo este proyecto, se hace uso de un servicio de confianza cualificado, el cual cumple los requisitos aplicables establecidos en el Reglamento (UE) 910/2014 [2] y que ayuda a la verificación y validación de firma electrónica y sellos electrónicos.

Con ayuda de uno de estos servicios, como es TrustedX de SafeLayer, se impulsa el cumplimiento de la normativa eIDAS, por el cual se implanta un flujo de autenticación por el protocolo estándar oauth2 y la verificación de certificado de un firmante. Todo esto junto a los servicios de almacenamiento en la nube, como Google Driver y Dropbox, se desarrolla la plataforma de firma documental.

Con ayuda de esta plataforma podemos realizar una firma digital, sin ninguna instalación de software, y tras realizar una serie de autenticación que nos valide como persona física y única.

1.2 Objetivos del Trabajo

El objetivo de este proyecto es la unificación de varios servicios entre los que cabe el almacenamiento en la nube y autenticación segura, para la ejecución de una firma electrónica en documentos PDF, sin la necesidad de una instalación de software de terceros.
La autenticación se realiza mediante estándares Oauth2 [3] que proporciona flujos simples de autorización específicos para plataforma y el embebido de varios proveedores de servicios cloud, donde se almacenará los documentos.

Con ayuda del servicio de firma cualificada TrustedX de Safelayer se lleva a cabo la autenticación del firmante en el dominio sobre el que se realizará la firma y donde se almacenará el certificado utilizado para la posterior firma digital.

Se debe tener en cuenta que para este TFM se dedicará un sistema demostrador de TrustedX conforme a la normativa eIDAS pero cuyo certificado de referencia no está cualificado. Además, la funcionalidad que presenta este demostrador para la firma de documentos no es real, puesto que para elevar el nivel de autorización en entorno real requeriría una clave que permite verificar la presencia de un usuario. En este TFM la clave será creada mediante el envío de un certificado pkcs#12 al servicio y, por tanto, la elevación de autorización solo se realizará confirmando el permiso de firma.
Esta diferencia no tiene cambio alguno en esta plataforma tan solo cambiaría el flujo de requerimientos que hace el servicio TrustedX contra el usuario.

Para el flujo de firma electrónica hace uso de los proveedores cloud para la descargar de un documento y posterior firma con ayuda del servicio TrustendX. Estos documentos firmados no se almacenarán en ningún servidor local, solo exclusivamente en el proveedor utilizado, de esta forma se guarda la privacidad documental del usuario.

Se promueve un diseño minimalista, sencillo e intuitivo para cualquier tipo de usuario. Por ello se forma un front-end utilizando el estándar de Bootstrap con una visualización limpia y espaciosa.
En base a la seguridad perimetral de este servicio hay que tener en cuenta tipos de ataque que pueden llevar a una violación de la identidad. Para ello se utiliza siempre comunicación cifrada tanto a cara del usuario final como la expuesta a cada proveedor de servicio.

1.3 Enfoque y método seguido

La evolución de este proyecto se lleva a cabo mediante una serie de etapas tomadas en cuenta a nivel general y en los cuales se puede apreciar una mayor delimitación del contenido.
En cada una de la fase se debe tener en cuenta las anteriores, puesto que su desarrollo es cronológico y estratégico.

Fase 1: Toma de requisitos y planificación

En esta fase se planifica la estimación del resto de tareas y se realiza la toma de todos los requisitos de información que se vaya a utilizar en el proyecto.

Fase 2: Análisis de los requisitos

Para esta tarea se realiza el análisis detallado de cada requisito, se define su desarrollo y su fin.

Fase 3: Desarrollo de requisitos

En este punto se comienza la implantación a nivel de sistema operativo, se definen métodos de seguridad perimetral, servicios aplicados y configuraciones a tener en cuenta para el soporte de la plataforma.

Fase 4: Desarrollo software

Esta fase es exclusiva para el desarrollo de la aplicación, donde se debe realizar el flujo entre los diferentes proveedores.

Fase 5: PenP (Puesta en producción)

Se elabora pruebas prácticas para una implantación desde cero. Se pretende el uso de Docker para facilitar el traspaso.

Fase 6: Documentación

Se define todos los términos, diagramas y flujos que se desarrollan en la aplicación. Además, se debe explicar cada paso dado a nivel de sistema operativo.

1.4 Planificación del Trabajo

Se define el siguiente diagrama de GANTT donde se detalla la evolución del proyecto.

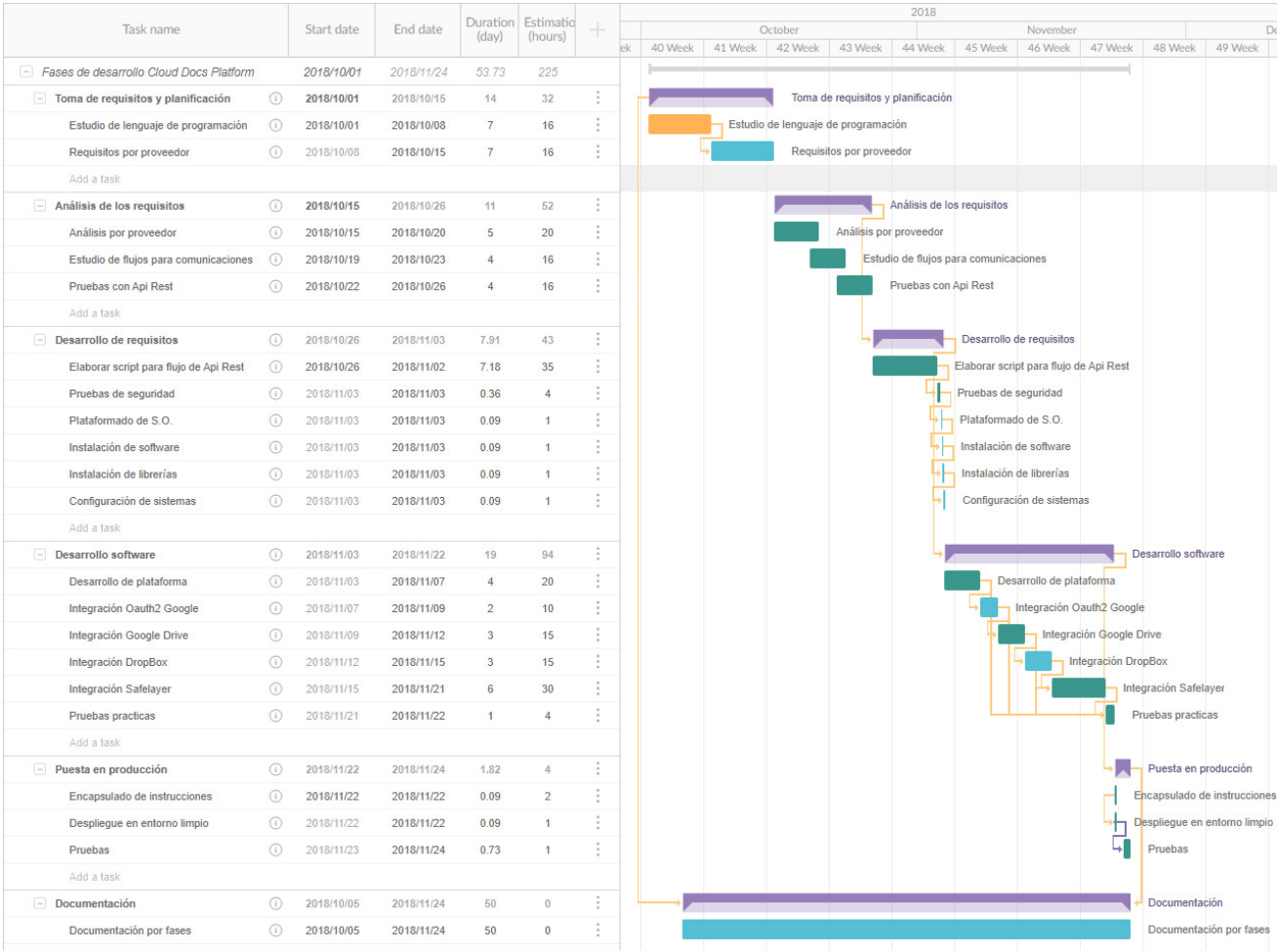


Figura 1: Diagrama de GANTT

1.5 Breve sumario de productos obtenidos

En cada uno de los capítulos que se llevara a cabo en este proyecto puede contener más de un hito. Puesto que la diferencia de cada etapa se delimita por el contenido específico. Pero como tal se mencionó, cada fase es dependiente de su anterior para poder proseguir en el tiempo.

1.6 Breve descripción de los otros capítulos de la memoria

Análisis de requisitos

Se evalúa todos los requisitos que dan soporte al aplicativo. El cometido es recaudar toda la información necesaria para posteriormente implementar en las siguientes tareas.

Arquitectura

Se detalla la interconexión entre la plataforma y los diferentes proveedores en los que se apoya.
Esta arquitectura se desarrolla en vista a la aplicación, pero no como una vista de sistema, puesto que se considera un sistema altamente escalable y por consiguiente todo servidor seguiría los mismos rasgos.

Diseño

Engloba todas las características que anteriormente se ha estudiado, así como su mecanismo y flujo de operatividad.

Implementación

En este punto se lleva a cabo el desarrollo de la plataforma utilizando todo los términos y nociones previstas.

Conclusión

Se explica un breve resumen de este proyecto y como se puede llegar a mejorar.

Glosario

Se define todo acrónico expuesto en este documento, a nota informativa y descriptiva.

Bibliografía

Apartado donde se procede a la mención de la documentación útil para este proyecto.

Anexos

Mención a los diferentes documentos agregados a este mismo proyecto.

2. Arquitectura

2.1. Descripción general

En esta primera toma de contacto se presenta una estructura que se tomará como boceto genérico y desde el cual se desarrollará todo el entorno.
Este desarrollo toma tres módulos diferentes cuya funcionalidad identifica su finalidad:

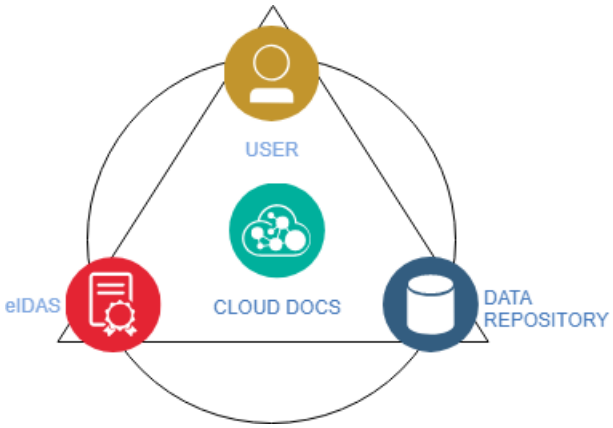


Figura 2: Módulo estático

En primer lugar, se presenta el módulo “USER” cuya lógica reside en la interacción con servicios IdP. En siguientes descripciones se mostrará su funcionalidad.
Después tenemos el módulo “DATA REPOSITORY”. Aquí se engloban los diferentes proveedores de almacenamientos existentes como puede ser Google Drive, Dropbox, Box, etc. Para este módulo es necesario disponer de un IdP en cada compañía y por el cual verificaremos el acceso y permisos especiales.
Por último, está el módulo eIDAS, llamado así por el Reglamento europeo que le hace referencia (*Electronic Identification and Authentication Services*), recoge todos los servicios electrónicos de confianza. Para este caso, se utiliza el servicio TrustedX de la empresa Safelayer.
Para este módulo, se hace necesaria también la funcionalidad de IdP disponible en cada servicio de confianza, para la verificación de acceso e identidades, así como, un proveedor de almacenamiento que se utiliza para la toma de un archivo pdf y posterior firma electrónica.

Estos tres módulos se relacionan entre sí para conformar la plataforma definitiva.

2.2. Descripción modular

En este apartado se procede a la descripción en más detalle de cada uno de los módulos expuestos y su funcionalidad.

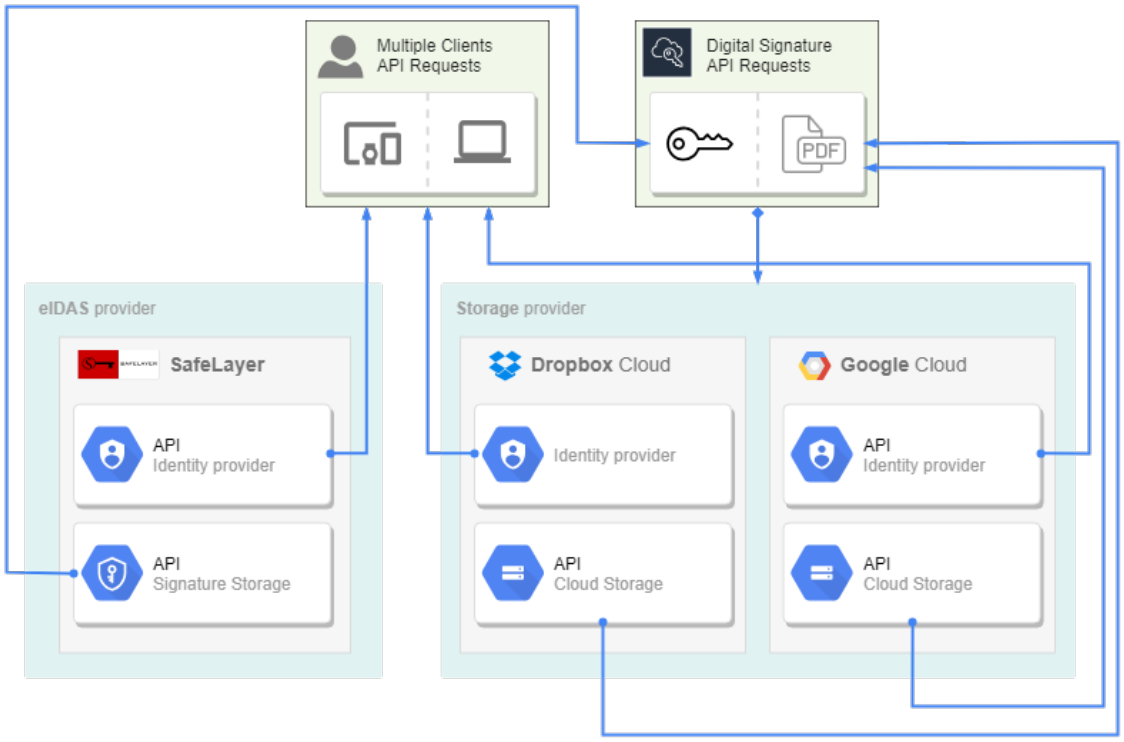


Figura 3: Diagrama de arquitectura

El ámbito de la arquitectura para este proyecto se encuadra en la implementación de un mínimo de una empresa de almacenamiento en la nube, mínimo de un proveedor de identidades (según reglamento eIDAS) y acceso mediante protocolo Oauth2 de un IdP.

Se procede con la implantación de llamadas a las API que proporcionan dos empresas de almacenamiento en la nube como son DropBox y Gloogle Drive, una empresa con características de identidad segura y tecnología de transacciones seguras como es Safelayer, y un IdP de autenticación para el acceso al portal.

De tal modo que en conjunto se realiza un flujo de trabajo que empieza con una identificación sobre el portal, aprovechando un IdP como es la API de Google Identity Platform [4], se navegará hacia uno de los proveedores eIDAS implantados, como es Trustedx de Safelayer, donde el usuario se identificará para cargar una nueva identidad y seleccionar para una posterior firma digital.
Un usuario autenticado en el proveedor eIDAS puede subir una nueva identidad bajo una categoría a seleccionar, puede eliminar una identidad existente y puede/debe seleccionar una identidad.

Una vez el usuario ha seleccionado una identidad, puede identificarse en uno o varios proveedores de almacenamientos en la nube.

En esta situación se puede descargar un fichero PDF existente en la nube o realizar una firma digital conforme a la identidad seleccionada de cada proveedor de identidad. Con esto se quiere decir que puede coexistir más de una identidad seleccionada, siempre y cuando sea de proveedores diferentes. En el proceso de dicha firma digital, el usuario podrá seleccionar que proveedor de identidad quiere que firme su documento PDF.
Una vez que el documento ha sido firmado se sube automáticamente al almacenamiento en la nube del proveedor escogido.

Haciendo esto conforme, los conjuntos importantes en este desarrollo dependerán de la gestión de ficheros, Gestión eIDAS y gestión de firma electrónica, y además como la autenticación a la Api de Google Identity sobre el protocolo Oauth 2.0.

2.3. Proveedor de identidad (IdP)

Un proveedor de identidad (IdP)[5], es un servicio en línea que autentica a los usuarios de Internet mediante tokens de seguridad. Los más destacados son Oauth2, SAML 2.0 y OpenID.

	SAML 2.0	**OAuth2**	**OpenID Connect**
What is it?	Open standard for authorization and authentication	Open standard for authorization	Open standard for authentication
History	Developed by OASIS in 2001	Developed by Twitter and Google in 2006	Developed by the OpenID Foundation in 2014
Primary use case	SSO for enterprise apps	API authorization	SSO for consumer apps
Format	XML	JSON	JSON

Figura 4: Diferencia de protocolos [11]

Los servicios de los que se hace uso disponen de un protocolo Oauth2 junto con una base de OpenID, de esta forma se obtiene un protocolo con doble servicio, por un lado, estaría el servidor de autorización y por otro el servidor de autenticación, el cual puede hacer uso de SSO para mantener a un usuario logado mientras la sesión en el servicio este activa.

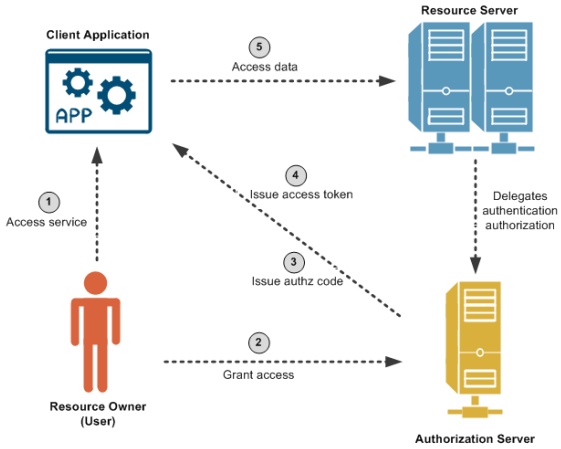


Figura 5: Diagrama Oauth2

2.3.1. Protocolos de autenticación

2.3.1.1. OpenID

Una de las bases de las cuales depende el protocolo Oauth es, OpenID. Un modelo de dominio asociado a OIDC.
Un proveedor de identidad puede confirmar la identificación OpenID del usuario a un sitio que soporte este sistema. Un detalle a tener en cuenta de este servicio es que a diferencia de otras arquitecturas Single Sign-On, OpenId no especifica el mecanismo de autenticación. Por lo tanto, la seguridad de una conexión OpenId depende de la confianza que tenga el cliente OpenID en el proveedor de identidad. [6]

2.3.1.2. Oauth2

Oauth2 es un protocolo estándar que permite un flujo de autorización segura para diversos tipos de aplicaciones. Este protocolo puede compartir información desde un proveedor a un usuario mediante una API [7][8].

2.3.2. Protocolos de autenticación implantados

Se procede a detallar el protocolo de autenticación en cada uno de los módulos.

2.3.2.1 Autenticación de la plataforma

Para este proyecto se implementa una autenticación mediante protocolo oauth2 hacia el proveedor Google Identity Platform.

Haciendo uso de este medio social, podemos conseguir un plus de seguridad puesto que no se almacena ningún dato personal en la plataforma.

Hoy en día hay multitud de proveedor identificación social, por ejemplo, Facebook, LinkedIn, Microsoft, etc que ponen a disposición una API para realizar una comunicación sencilla con el servicio.

2.3.2.1.1 Google Identity Platform

Este proveedor proporciona los medios necesarios para una autenticación seguro a la plataforma de cualquier usuario con una cuenta en Google.

La plataforma Cloud Docs hará uso de varios de datos del usuario logado:

Permiso	Extensión
Consulta de email	https://www.googleapis.com/auth/userinfo.email
Consulta de Perfil	https://www.googleapis.com/auth/userinfo.profile

Con estas extensiones la plataforma consigue los siguientes datos de un usuario:

Referencia	Descripción
family_name	Muestra solo el apellido
name	Muestra el nombre con apellidos

picture	Muestra la URL de la imagen avatar
locale	Muestra la nacionalidad
email	Muestra el email
link	Muestra la URL del perfil de Google+
given_name	Muestra solo el nombre
id	Muestra el id del usuario Google
verified_email	Boolean indicando el estado de la cuenta

Con este conjunto de datos, Cloud Docs puede autenticar y hacer un perfil del usuario conectado.

2.3.2.2 Autorización en proveedores

Cada proveedor tiene su propio IdP para asegurar una comunicación segura e identificativa de cada usuario con sus datos y contenido personales.

2.3.2.2.1 Google Drive

Para el proveedor Google Drive se realiza una petición Oauth2 sobre el mismo el IdP de Google Identity Platform, pero en este caso las extensiones utilizadas serán diferente. Estas extensiones(scope) estarán referenciadas a la API Google Drive, por las cuales un usuario autoriza el acceso a su contenido y modificación del cual.

Permiso	Extensión
Leer, editar, escribir y eliminar ficheros	https://www.googleapis.com/auth/drive
Ver y administrar metadatos de ficheros	https://www.googleapis.com/auth/drive.metadata

Gracias a estos permisos que otorga el usuario a la plataforma Cloud Docs, se podrá acceder a una lista de ficheros PDF contenido en el almacén de Google Drive, tras los cuál se puede descargar o subir ficheros firmados.

Se detalla el permiso a los metadatos para poder obtener sin problemas el nombre de los ficheros o para saber si un fichero es compartido con otros usuarios de google.

2.3.2.2.2 DropBox

Este proveedor dispone de un proceso de autenticación Oauth2 al igual que el resto de los proveedores implantados, pero, con la única diferencia que, no utiliza extensiones para los permisos sobre el contenido.

La API de DropBox solo permite detallar algunas opciones referentes a permisos como son las opciones de sobre escritura de un fichero o la generación de uno nuevo cuando se llama a las funciones determinadas para creación o subida de ficheros.

2.3.2.2.3 TrustedX

TrustedX [15] dispone de una API segura por la cual se conecta el portal mediante protocolo Oauth2. Este servicio, al igual que los demás servicios de autenticación implantados, ofrecen una base OpenID. Por la cual el usuario

puede interactuar con el proveedor con solo introducir las credenciales una primera vez. Es decir, utiliza el funcionamiento SSO para mantenerlos logados en su IdP, y solo haría falta que le usuario pasase por el servidor de autorización “AuthServer” para dar el consentimiento.

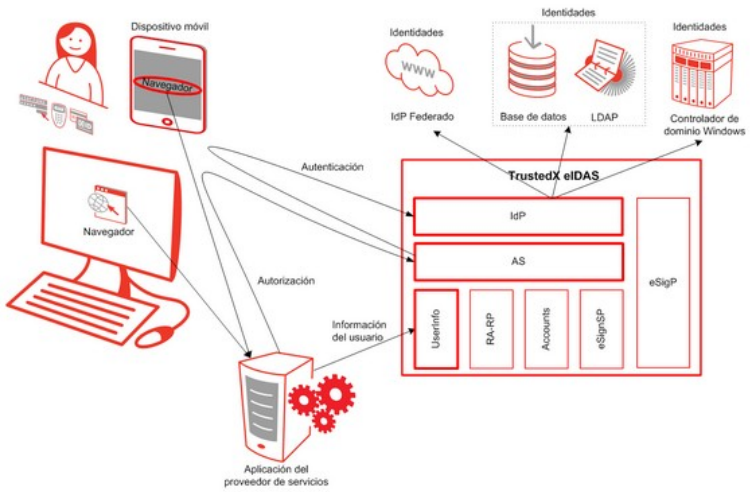


Figura 6: Diagrama Oauth2 TrustedX

El protocolo de Oauth2, al igual que Google Identity, hace uso de Authorization Code Grant (RFC6749) por la cual podemos realizar la petición de un token con los permisos deseados mediante un código (code) alfanumérico proporcionado por el servicio.

Se debe saber que este token con una duración determinada será gestionado por el portal Cloud Docs para así, mantener una linea de actividad contra el servicio TrustedX.

La petición de autenticación debe llevar consigo las siguientes extensiones:

Permiso	Extensión
Registrar identidades de firma	urn:safelayer:eidas:sign:identity:register
Gestionar identidades de firma	urn:safelayer:eidas:sign:identity:manage

Una vez que el usuario autoriza estas extensiones la plataforma tiene el consentimiento de ver, editar, agregar y eliminar una identidad en la cuenta de TrustedX del usuario.

2.4. Proveedor de almacenamiento

Este tipo de proveedores prestan un servicio de almacenamiento en la nube. Los cuales se destacan por su habilidad y facilidad de acceso para los números documentos de un usuario.
Los proveedores de almacenamiento contienen, aparte de una gestión importante de ficheros, un IdP, mencionado anteriormente. Con esta autenticación podemos conseguir que la plataforma del proveedor nos responda a diferentes acciones. Esto se lleva a cabo gracias a la implantación

de una API Rest del proveedor, por la cual se produce un flujo seguro desde una aplicación consumir.

2.4.1. Google Drive

Este proveedor da un servicio de almacenamiento a todo usuario con una cuenta Google. Gracias a su API Rest y los permisos, de los cuales hemos hablado anteriormente, la plataforma puede consultar la lista de ficheros, descargar y subir.
La plataforma solo realiza peticiones de listar los documentos pdf mediante un filtro Mime en la propia petición.

A nivel técnico, antes de que el portal requiera cualquier permiso al usuario, debe existir una aplicación configurada en el proveedor. Esta aplicación no quiere decir que se realice un desarrollo sino una petición de acceso para que el portal tenga autorización a los datos mediante los permisos otorgados por un usuario.

Además, y puesto que Google tiene diversos servicios en cloud, se debe de da alta el servicio a utilizar. En este caso Google Drive.

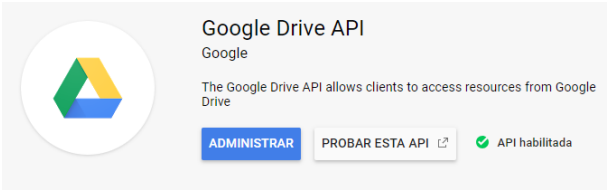


Figura 7: API Google Drive

Con todo configurado en la plataforma de GoogleAPIs se puede llevar a cabo el siguiente proceso general que se puede aplicar a todos los tipos de aplicaciones [9]:

1. Crear y registrar la aplicación usando la Consola API de Google. Google proporciona la información necesaria, como una identificación de cliente y un secreto de cliente.
2. Activar la API de Drive en la consola de la API de Google.
3. Configurar el alcance que deba tener el portal, para requerir los permisos a Google.
4. Google muestra una pantalla de consentimiento para que el usuario autorice a la aplicación solicitar los datos requeridos.
5. Si el usuario lo aprueba, Google devuelve un code haciendo uso del término Authorization Code Grant.
6. El portal tramita la petición de un token de corta duración con Google.
7. A continuación y a petición del usuario, el portal solicita datos de usuario, adjuntando el token de acceso a la solicitud.
8. Si Google determina que su solicitud y el token son válidos, entonces se pueden ejecutar las acciones de descarga, subida o listado de ficheros.

Con todas estas comunicaciones y peticiones GoogleAPIs elabora unas estadísticas donde se observa el comportamiento con el portal.

Figura 8: Panel de administración Google Drive

2.4.2. Dropbox

Este proveedor, al igual que Google Drive, aporta un servicio de almacenamiento en la nube.
El usuario interactúa igual que con los demás proveedores. Debe dar permisos para a autorizar al portal en la recolecta de datos. Estos permisos los da a través de una interfaz SAML 2.0 que entrega Dropbox al usuario.

Para que el portal Cloud Docs pueda obtener los permisos de los usuarios con cuenta en DropBox, se ha configurado una aplicación, al igual que se realiza en Google Drive.

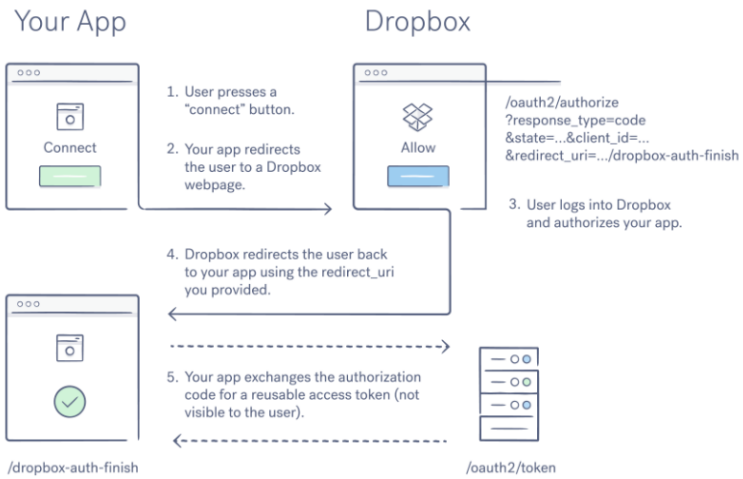


Figura 9: Diagrama Oauth2 DropBox

La configuración de dicha aplicación tiene un detalle que Google Drive lo realiza mediante las extensiones (scope). Dropbox pide al administrador, es decir al creador de dicha aplicación, que informe si las actuaciones sobre los usuarios (lectura, descarga, subida o modificación de ficheros) se hará sobre todo el contenido disponible del usuario o exclusivamente sobre una carpeta.
En este portal, se realiza una petición de listado sobre todo el contenido de un usuario, puesto que la búsqueda de un documento puede ser más simple e intuitiva.

En esta configuración, Dropbox aporta los datos suficientes para que e portal pueda tener acceso a la aplicación y así poder conseguir las autorizaciones que los usuarios aprueben. Esta autorización le viene dado al portal mediando un token con una caducidad determinada, actuación que desempeña el protocolo Oauth2 de Dropbox.

2.5. Proveedor eIDAS

Para este proyecto se hace necesario por su finalidad tener al menos un proveedor de identidades que cumpla con el reglamento eIDAS, cuyo hito fundamental que se busca en ello es la legalidad de la firma electrónica en Europa.

La implantación del proveedor debe tener la característica para poder realizar una firma asíncrona y así poder, Cloud Docs, ejecutar la actividad de firma dentro del estándar PAdES [14] que especifica los perfiles precisos que debe cumplir con la normativa europea eIDAS.

La firma asíncrona es necesaria para esta funcionalidad, puesto que la plataforma Cloud Docs no almacena ningún certificado privado. La terminología asíncrona, se debe a que la firma consta de dos partes fundamentales. En la primera parte se realizar un despiece del pdf donde aglomeran los datos a firmar y de los cuales se extrae un hash que se envía al proveedor de identidades para que sea firmado por la clave privada de la identidad del usuario. Y en la segunda parte, se compacta dicho hash firmado y el certificado público de la identidad. Así pues, cuando el software de lectura procese el documento pdf, realizará un diagnóstico de la firma contra el hash del documento original, y verificará la firma digital y la no permutabilidad del fichero. Más adelante se hablará más técnicamente de este proceso de firma.

2.5.1. TrustedX

El proveedor TrustedX, de la empresa Safelayer que proporciona la funcional perfecta para la solución que se busca en este proyecto. Por medio de la API Rest de que dispone TrustedX se realiza la gestión de los procesos de firma electrónica.

Como hablamos anteriormente, este servicio, contiene un IdP propio para la autenticación de los usuarios en la plataforma y cuya comunicación se realiza mediante protocolo Oauth2. El cual le permite al portal Cloud Docs obtener los

permisos necesarios para poder obtener los datos necesarios sobre las identidades del usuario.

La funcionalidad que implementa Cloud Docs sobre este proveedor de identidades, abarca la siguiente gestión:
- Un usuario podrá eliminar uno o más identidades de su almacén.
- Un usuario podrá agregar su certificado al repositorio eSigP de TrustedX.
- Un usuario podrá firmar un documento PDF mediante una de sus identidades firmantes.

En el siguiente diagrama se puede observar a modo de ejemplo la trazabilidad que se realiza para agregar una identidad, que el usuario sube, a TrustedX.

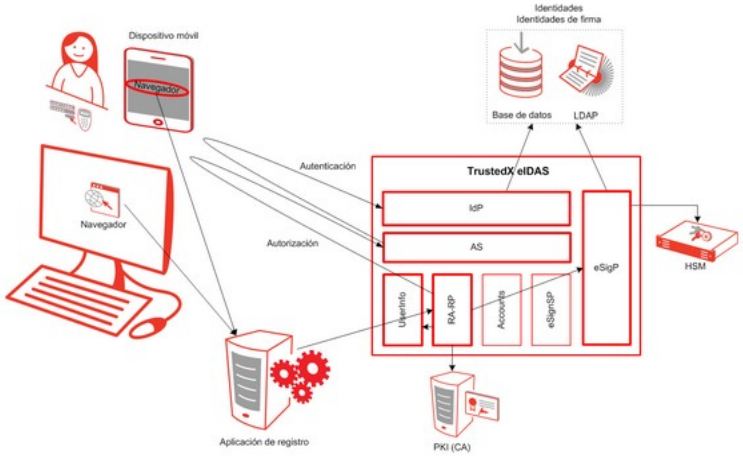


Figura 10: Diagrama de gestión de identidad TrustedX

Remarcando uno de los puntos importantes; la firma electrónica sobre un documento PDF.
El dialogo con TrustedX para realizar una firma, empieza realizando una llamada a su IdP mencionando una extensión diferente a las utilizadas en anteriormente. Esta extensión y junto a una identidad que el usuario haya seleccionado se realiza una petición de Authorization Code Grant bajo el protocolo Oauth2, y por el cual obtenemos un token con el permiso del usuario para la firma del documento.

Permiso	Extensión
Uso de identidades	urn:safelayer:eidas:sign:identity:use:server

Tras esta actuación, cloud Docs empieza a trabajar sobre el documento, que anteriormente el usuario ha tenido que elegir, realizando una serie de puntos hasta que el documento quede firmado.

La firma electrónica del documento no trata de firmar todo su contenido, sino que, realiza una firma del hash extraído del documento original y por el cual se asegura que el documento no tenga ninguna modificación.
Esta es la técnica que se utiliza para conformar con el marco PadES, un estándar con base CadES.

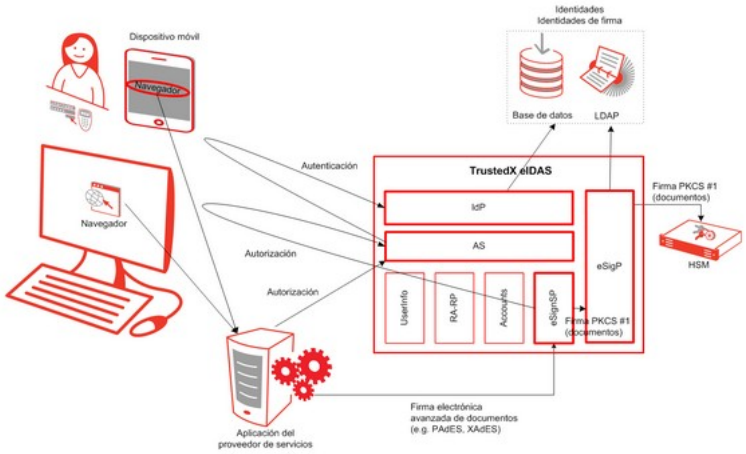


Figura 11: Diagrama de firma electrónica TrustedX

En este diagrama, se observa la trazabilidad de la firma electrónica.
Aquí, intervienen dos de los componen que conforman el núcleo del proceso, estos son, eSigP y eSignSP.

eSignSP: Es el componente que proporciona un servicio de firma electrónica de documentos.

eSigP: Es el componente que guarda la identidad del usuario y realiza la firma en base al hash del documento.

El portal Cloud Docs actuaria directamente sobre el componente eSigP, pues el propio servidor ya se encarga del cálculo del hash. En resumen, Cloud Docs consulta a TrustedX la identidad de la firma y envía el cálculo del hash cuyo resultado será un hash firmado por esa identidad del usuario.
Esa firma la introduce Cloud Docs en el documento y a continuación lo presenta a uno de los proveedores de almacenamiento elegido por el usuario.
De este modo y haciendo conforme la autorización del usuario para la manipulación de ficheros por cloudDocs, el documento no sale del ámbito de la aplicación.

2.6. Autorización de firma electrónica

Este TFM defiende uno de los hitos más importante que es la firma electrónica cualificada y autorización del servicio eIDAS para el firmado de documentos.
Existen dos tipos más de firma electrónica que no se utilizará, pero se debe tener conciencia de ello:

	Firma electrónica simple	Firma electrónica avanzada	Firma electrónica cualificada
Facilidad	✔	✔	
Seguridad		✔	✔
Legalidad		✔	✔
Necesidad de dispositivos			✔

- La firma electrónica simple es fácil de implantar, pero difícil de verificar puesto que no verifica quien ha sido su firmante.

- La firma electrónica avanzada tiene mayor nivel de seguridad que la simple y ofrece mayor seguridad, confirmando que el firmante es quien dice ser y limitando el riesgo de suplantación. Este tipo de firma está aprobada para evidencia jurídica.

- La firma electrónica cualificada o firma reconocida, hace uso de un certificado cualificado y un servidor protegido HSM que cumpla con las características que describe el Reglamento EU 910/2014.

El tipo de firma que se realiza para este proyecto es la firma electrónica cualificada puesto eleva el nivel d seguridad para la plataforma y para ello se requiere de un servidor protegido para llevar a cabo el flujo de la firma.

En esta ocasión se dispone del servicio TrustedX, pero como se comentó en la introducción es un servicio demo para mostrar su funcionalidad. La diferencia que existe entre el entorno demo y un entorno productivo es el certificado y el tipo de autorización.
El certificado utilizado para realizar la firma electrónica no es un certificado cualificado, por tanto, se debe introducir en los diccionarios de confianza un certificado raíz que verifique el certificado de la firma correctamente.
Por otro lado, el tipo de autorización que se realiza contra la demo cambia respecto a un entorno real. Se debe generar una clave única para un usuario que debe hacerlo el proveedor de firma protegido por un HSM, pero en este caso, se genera una clave mediante un certificado pkcs#12 que se sube directamente al servicio de TrustedX. Con esto se produce que, al autorizar la firma de un documento, el servicio de TrustedX eSigP no requiera de una clave para confirmar la identidad, en cambio solo exige autorizar el permiso de firma electrónica. Con esta acción el servicio eleva la autorización y procede al firmado del hash enviado por la plataforma.

Estas dos peculiaridades del servicio TrustedX no conlleva ningún cambio en la plataforma puesto que la autorización y firma electrónica se realiza entre el usuario y el servicio eIDAS. La plataforma solo recoge los datos firmados para armar el documento PDF.

2.7. Firma electrónica

Este proyecto se fundamenta en el hito de la firma electrónica de documentos PDF mediante una identidad de persona física. Esta firma se realiza con el estándar PAdES [14] que especifica el perfil necesario para cumplir con la normativa europea eIDAS.

El estándar PAdES (ETSI TS 102 778 [12]) perfila el soporte para firmas digitales del formato PDF 1.7 (ISO 32000-1) con la finalidad de poder incluir firmas electrónicas avanzadas en los documentos PDF.

El desarrollo de este estándar se realiza con ayuda de uno de los proveedores eIDAS de que el portal dispone, por el cual obtenemos una firma del hash del documento. Esta firma verifica que el documento no ha sido cambiado tras su firma.

Dicha firma (ISO 32000-1 [13]) permite realizar tres actividades: agregar una firma digital a un documento, proporcionar un campo de marcador de posición donde irán las firmas, y verificar la validez de las firmas.

La estructura de datos de un PDF contiene un apartado llamado diccionario de firmas, donde se encuentra la firma codificada como un objeto binario utilizando CMS (Cryptographic Message Syntax) o el formato relacionado PKCS#7; un resumen del cálculo hash sobre un rango de bytes del archivo, una identidad con clave publica y una estampa de tiempo.

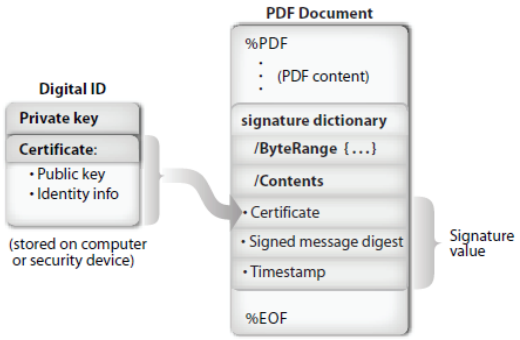


Figura 12: Contenido cifrado en un PDF

El tamaño del rango se calcula en función de la mejor estimación del tamaño máximo necesario para contener la firma del PDF y cualquier revocación adicional e información de sellado de tiempo.
La primera traza que compone la estructura de contenido es una cadena con una serie de valores hexadecimales 0x00 que rellenan el campo y una vez calculada la firma, se completa con el contenido real.

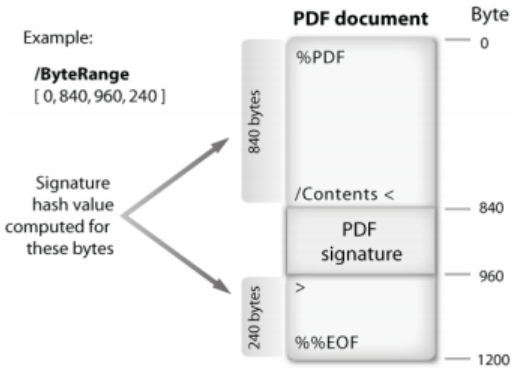


Figura 13: Calculo del hash de un PDF

Así pues, si se considera hacer más de una modificación en el documento y su posterior firma, el hash a calcular viene dado por los siguientes rangos, según la cantidad de firmas.

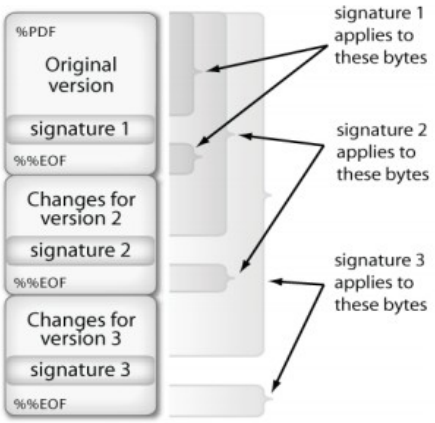


Figura 14: Calculo de hash de un pdf en cascada

Este cálculo del hash es enviado al proveedor eIDAS seleccionado para su posterior firma según la identidad escogida.
Dicha firma se recepciona en formato PKCS#7 que se unirá junta a la identidad, sello de tiempo y disposición del sello en el documento.

Una buena técnica para el sellado de tiempo es hacer uso de los servidores de sellado de tiempo confiable (TSA) (RFC3161) a través del Time-Stamp Protocol (TSP).

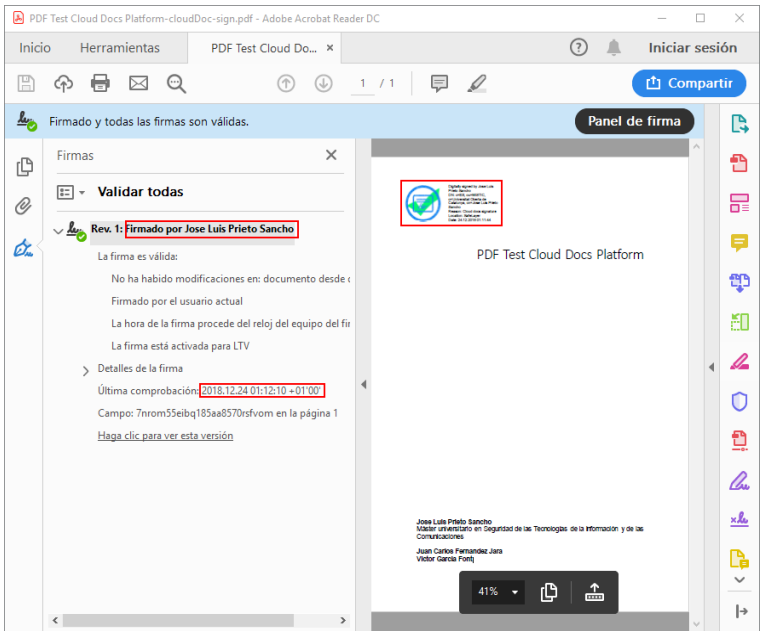


Figura 15: PDF firmado digitalmente

3. Análisis de Requisitos

3.1. Diagrama de análisis estático

Se presenta el siguiente diagrama DAE. Este esquema depende de un núcleo como es un usuario de la red.
Para la toma de requisitos siguientes se tiene en cuenta que puede existir más de un proveedor de almacenamiento en la nube, como es Google Driver o Dropbox, y también más de un proveedor eIDAS, como es TrustedX de Safelayer.

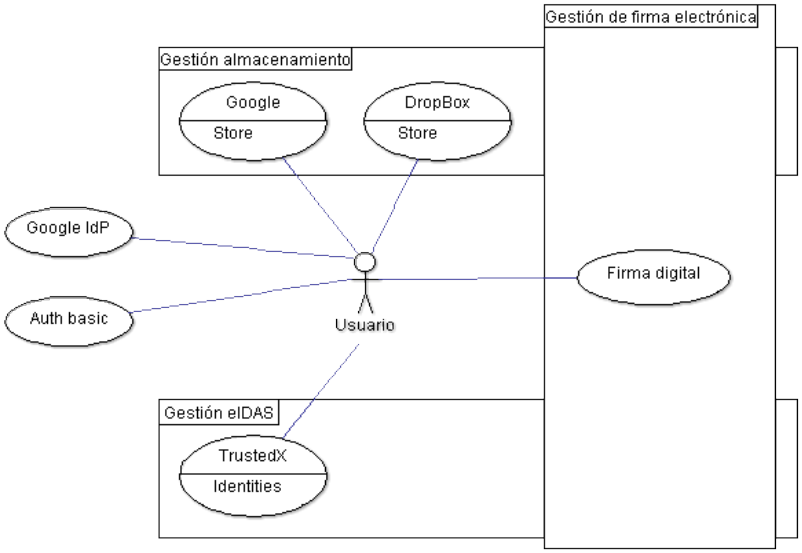


Figura 16: Diagrama de estado

3.2. Actuadores

ACT-0001	**Usuario**
Descripción	Este actor representa a uno de los usuarios comunes
Comentarios	Puede utilizar la aplicación por la cual se comunica con la red

ACT-0002	**CloudDocs**
Descripción	Este actor representa el portal
Comentarios	Ninguno

ACT-0003	**Proveedor eIDAS**
Descripción	Este actor representa a un proveedor eIDAS. Por ejemplo, Safelayer
Comentarios	Ninguno

ACT-0004	Google Identity
Descripción	Este actor representa a la API de Google Identity
Comentarios	Ninguno

ACT-0005	Proveedor de almacenamiento
Descripción	Este actor representa a un proveedor de almacenamiento en la nube
Comentarios	Ninguno

3.2. Objetivos específicos

OBJ-0001	Firma digital
Descripción	El sistema podrá descargar, firmar y subir un fichero PDF a una de las plataformas en la nube donde el usuario haya dado su consentimiento de acceso y gestión.
Subobjetivos	**[OBJ-0015] Seleccionar una identidad**: Un usuario deberá seleccionar una de sus identidades de un proveedor eIDAS
Comentarios	Ninguno

OBJ-0003	Inicio de sesión Google
Descripción	El sistema pedirá consentimiento de logado a una cuenta Google ofrecida por el usuario para acceder
Subobjetivos	**[OBJ-0006] Permisos Google Identity**: El sistema deberá pedir consentimiento al usuario con cuenta en Google para recibir datos de su perfil
Comentarios	Ninguno

OBJ-0004	Almacenamiento en la nube
Descripción	Un usuario podrá visualizar y descargar su contenido, con filtro PDF, en la nube.
Subobjetivos	**[OBJ-0007] Acceso a cloud**: El sistema deberá requerir un usuario ya registrado en el proveedor escogido.
	[OBJ-0008] Gestión de ficheros: El sistema deberá requerir permisos al usuario para gestionar sus ficheros de la plataforma elegida.
	[OBJ-0009] Listado de ficheros: El sistema podrá listar todos los ficheros, con filtro PDF, que el usuario tenga disponibles en proveedor elegido.
	[OBJ-0010] Descarga de ficheros: El sistema deberá poder descargar cualquier fichero, con filtro PDF, que el usuario tenga disponible en proveedor elegido.
Comentarios	Ninguno

OBJ-0005	eIDAS

Descripción	Un usuario podrá gestionar una cuenta eIDAS, agregando o eliminado identidades.
Subobjetivos	**[OBJ-0012] Acceso a proveedor eIDAS**: El sistema deberá requerir una cuenta de acceso al proveedor eIDAS con protocolo OAuth 2.0.
	[OBJ-0013] Gestión de identidades: El sistema deberá poder gestionar las identidades de los usuarios, para la posterior utilización en firmas digitales.
Comentarios	Ninguno

3.3. Requisitos de información

IRQ-0001	**Usuario Google**
Dependencias	[OBJ-0006] Permisos Google Identity
Descripción	El sistema realizará una petición de información correspondiente a un usuario Google.
Datos específicos	ID email Nombre Apellidos token
Comentarios	El sistema utilizará el registro de token mientras no haya caducado.

IRQ-0002	**Cuenta proveedor de almacenamiento**
Dependencias	[OBJ-0008] Gestión de ficheros
	[OBJ-0007] Acceso a cloud
Descripción	El sistema requiere de un usuario registrado en el proveedor de almacenamiento, por el cual se tendrá acceso a su gestión.
Datos específicos	ID token
Comentarios	El sistema utilizará el registro de token mientras no haya caducado.

IRQ-0003	**Cuenta proveedor eIDAS**
Dependencias	[OBJ-0013] Gestión de identidades
	[OBJ-0012] Acceso a proveedor eIDAS
	[OBJ-0001] Firma digital
Descripción	El sistema requiere de un usuario registrado para la gestión de identidades y la firma de documentos.
Datos específicos	ID dominio token
Comentarios	Ninguno

IRQ-0004	**Identidad**

Dependencias	[OBJ-0001] Firma digital
	[OBJ-0013] Gestión de identidades
Descripción	El sistema requiere de un certificado digital para la gestión de identidades y firma de documentos.
Datos específicos	etiquetas certificado clave pública ID
Comentarios	Ninguno

IRQ-0005	**Usuario CloudDocs**
Dependencias	[OBJ-0002] Inicio de sesión
Descripción	El sistema requiere de un usuario registrado para el acceso y por el cual se realiza una petición a base de datos.
Datos específicos	ID
Comentarios	Ninguno

3.4. Requisitos de restricción

CRQ-0001	**Ficheros**
Dependencias	[OBJ-0004] Almacenamiento en la nube
Descripción	El sistema realiza un filtrado de ficheros exclusivamente con formato PDF sobre todo el contenido de cualquier proveedor de almacenamiento
Comentarios	Ninguno

3.5. Casos de uso

UC-0001	**Inicio de sesión Google**	
Versión	1.0	
Dependencias	[IRQ-0001] Usuario Google	
Descripción	Un usuario con cuento en Google puede logar en el portal mediante la API Google Identity (Protocolo Oauth 2.0)	
Precondición	El usuario debe tener una cuenta en Google Account	
Secuencia normal	**Paso**	**Acción**
	1	El usuario (ACT-0001) realiza una petición de logado.
	2	El usuario (ACT-0001) es redirigido a Google Identity (ACT-0004), donde debe introducir sus credenciales y aprobar los permisos.
	3	El usuario (ACT-0001) da su consentimiento a Google Identity (ACT-0004)

	4	Google Identity (ACT-0004) responde con un atributo code
	5	CloudDocs (ACT-0002) pide a Google Identity (ACT-0004) un token en referencia al code
	6	Google Identity (ACT-0004) recibe code y devuelve un token
	7	CloudDocs (ACT-0002) almacena token
	8	CloudDocs (ACT-0002) pide a Google Identity (ACT-0004) datos del perfil
	9	Google Identity (ACT-0004) responde con datos del usuario
	10	CloudDocs (ACT-0002) presenta al usuario (ACT-0001) su perfil.
Postcondición	El usuario debe permitir el acceso a su información	
Excepciones	**Paso**	**Acción**
	3	Si el usuario rechaza los permisos, la acción queda sin efecto
Comentarios	Ninguno	

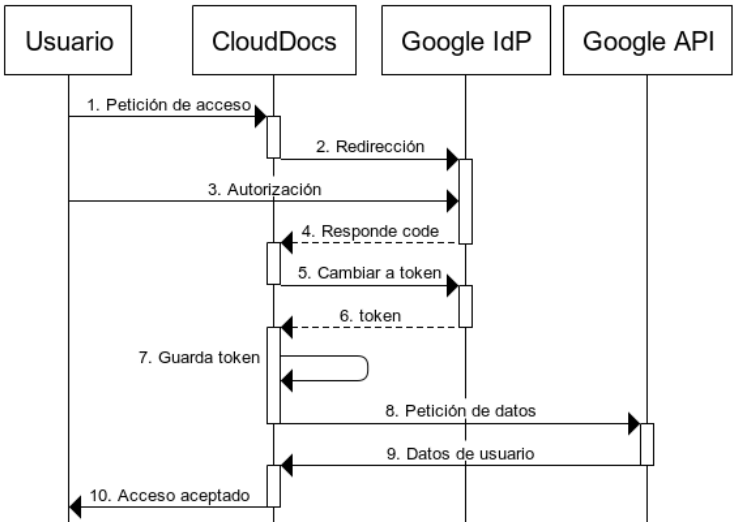


Figura 17: Caso: Inicio de sesión Google

UC-0002	**Listar ficheros Almacenamiento**	
Versión	1.0	
Dependencias	[OBJ-0007] Gestión de ficheros	
	[IRQ-0002] Cuenta proveedor de almacenamiento	
	[CRQ-0001] Ficheros	
Descripción	Un usuario puede listar sus ficheros PDF almacenados en el proveedor escogido.	
Precondición	El usuario debe tener una cuenta en el proveedor de almacenamiento en la nube	
Secuencia normal	**Paso**	**Acción**

	1	El usuario (ACT-0001) pide acceso a CloudDocs (ACT-0002)
	2	CloudDocs (ACT-0002) redirige al Proveedor de almacenamiento (ACT-0005)
	3	El usuario (ACT-0001) da su consentimiento al Proveedor de almacenamiento (ACT-0005)
	4	Proveedor de almacenamiento (ACT-0005) responde con un atributo code
	5	CloudDocs (ACT-0002) pide a Proveedor de almacenamiento (ACT-0005) un token en referencia al code
	6	Proveedor de almacenamiento (ACT-0005) recibe code y devuelve un token
	7	CloudDocs (ACT-0002) almacena token para el proveedor
	8	CloudDocs (ACT-0002) realiza una llamada a la API del Proveedor de almacenamiento (ACT-0005) para obtener un listado de ficheros PDF
	9	El proveedor de almacenamiento (ACT-0005) devuelve un listado con los nombres e identificadores de ficheros PDF
	10	CloudDocs (ACT-0002) presenta al usuario la lista de ficheros PDF
Postcondición		
Excepciones	**Paso**	**Acción**
	3	Si el usuario rechaza los permisos, la acción queda sin efecto
Comentarios	Ninguno	

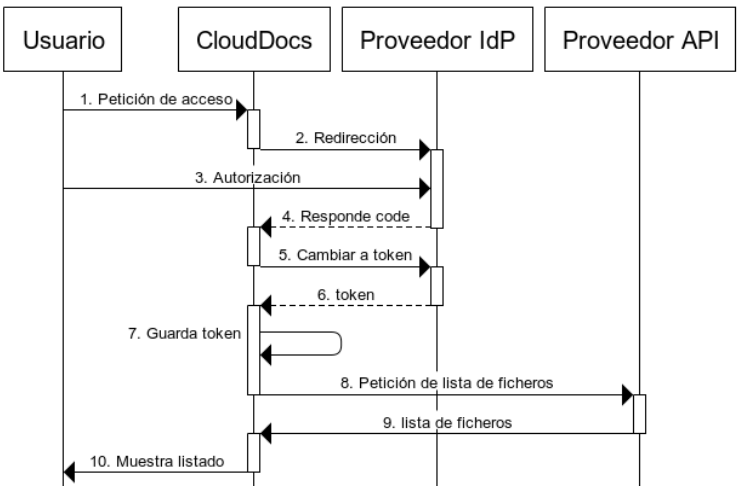


Figura 18: Caso: Listar ficheros

UC-0003	**Descargar ficheros Almacenamiento**
Versión	1.0
Dependencias	[OBJ-0007] Gestión de ficheros

	[IRQ-0002] Cuenta proveedor de almacenamiento	
	[CRQ-0001] Ficheros	
Descripción	Un usuario puede descargar sus ficheros PDF almacenados en el proveedor escogido, siempre y cuando el usuario haya permitido el acceso a sus ficheros.	
Precondición	[UC-0003] Listar ficheros Almacenamiento	
Secuencia normal	**Paso**	**Acción**
	1	El usuario (ACT-0001) pide descargar un fichero a CloudDocs (ACT-0002)
	2	CloudDocs (ACT-0002) comprueba que existe una sesión abierta con el Proveedor de almacenamiento (ACT-0002)
	3	CloudDocs (ACT-0002) envía al Proveedor de almacenamiento (ACT-0005) la petición de descarga
	4	Proveedor de almacenamiento (ACT-0005) devuelve a CloudDocs (ACT-0002) el fichero
	5	CloudDocs (ACT-0002) dispone el fichero para la descarga, al usuario (ACT-0001)
Postcondición		
Excepciones	Ninguno	
Comentarios	Ninguno	

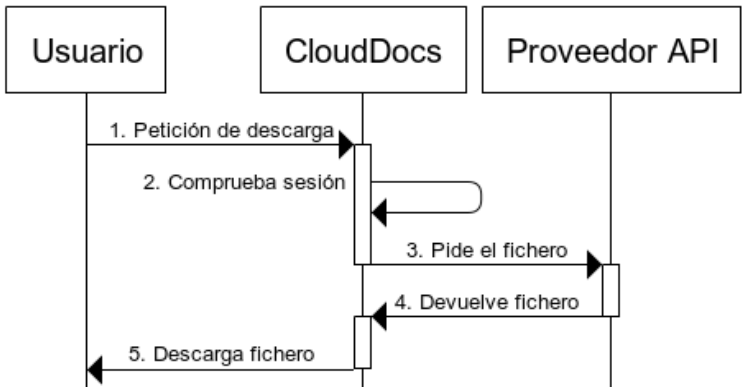


Figura 19: Caso: Descargar fichero

UC-0004	**Acceso cuenta eIDAS**	
Versión	1.0	
Dependencias	[IRQ-0003] Cuenta proveedor eIDAS [OBJ-0005] eIDAS	
Descripción	Un usuario pide logarse en un proveedor eIDAS disponible en el portal.	
Precondición	Disponer de un usuario valido para el proveedor eIDAS	
Secuencia normal	**Paso**	**Acción**
	1	El usuario (ACT-0001) pide acceso a CloudDocs (ACT-0002) para un proveedor eIDAS (ACT-0003)
	2	CloudDocs (ACT-0002) redirecciona al proveedor eIDAS (ACT-0003) con parámetro de etiqueta di-

		námica
	3	El usuario (ACT-0001) introduce las credenciales en proveedor eIDAS (ACT-0003)
	4	Proveedor eIDAS (ACT-0003) pide autorización al usuario (ACT-0001)
	5	El usuario (ACT-0001) da su consentimiento a Proveedor eIDAS (ACT-0003)
	6	Proveedor eIDAS (ACT-0003) responde con un atributo code
	7	CloudDocs (ACT-0002) pide a Proveedor eIDAS (ACT-0003) un token en referencia al code
	8	Proveedor eIDAS (ACT-0003) recibe code y devuelve un token
	9	CloudDocs (ACT-0002) almacena token
	10	CloudDocs (ACT-0002) realiza una llamada a la API del Proveedor eIDAS (ACT-0003) para obtener un listado de las identidades
	11	El proveedor eIDAS (ACT-0003) devuelve un listado de identidades
	12	CloudDocs (ACT-0002) presenta al usuario su información
Postcondición		
Excepciones	**Paso**	**Acción**
	3	Si el usuario rechaza el logado, la acción queda sin efecto
	4	Si el usuario no acepta los permisos, la acción queda sin efecto
Comentarios	Ninguno	

Para este caso se desarrolla un diagrama exclusivo para TrustedX de Safelayer puesta que por el momento es el único proveedor que se dispone.
TrustedX dispone de su servidor de almacenamiento de identidades llamado eSigP aparte de su IdP y servidor de autenticación que se presentan como TrustedX.

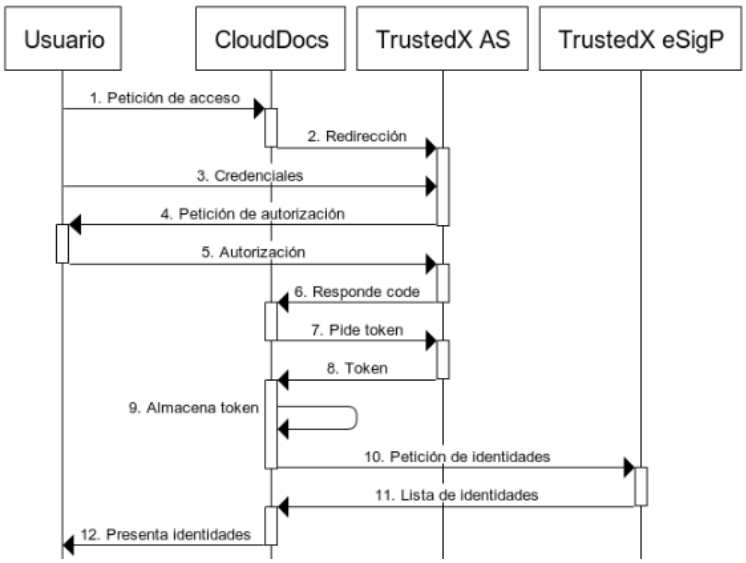


Figura 20: Caso: Acceso cuenta eIDAS

UC-0005	**Agregar identidad**	
Versión	1.0	
Dependencias	[IRQ-0003] Cuenta proveedor eIDAS [OBJ-0013] Gestión de identidades	
Descripción	Un usuario con acceso al proveedor eIDAS puede agregar un certificado p12 ofrecido por la empresa	
Precondición	El usuario debe tener una cuenta activa	
Secuencia normal	**Paso**	**Acción**
	1	El usuario (ACT-0001) realizar una petición para agregar nuevo certificado
	2	CloudDocs (ACT-0002) pide el certificado al usuario
	3	CloudDocs (ACT-0002) lee el certificado, etiqueta y password
	4	CloudDocs (ACT-0002) envía certificado, etiqueta y contraseña al proveedor eIDAS (ACT-0003).
	5	Proveedor eIDAS (ACT-0003) responde con una aprobación
	6	CloudDocs (ACT-0002) realiza una llamada a la API del Proveedor eIDAS (ACT-0003) para obtener un listado de las identidades
	7	El proveedor eIDAS (ACT-0003) devuelve un listado de identidades
	8	CloudDocs (ACT-0002) presenta al usuario (ACT-0001) su información
Postcondición	El certificado permite firma electrónica sobre un archivo PDF	
Excepciones	**Paso**	**Acción**
	3	El certificado o contraseña es incorrecto, la acción se queda sin efecto
Comentarios	Ninguno	

Igual que anteriormente se presenta un diagrama real para la comunicación entre CloudDocs y el servicio eSigP.

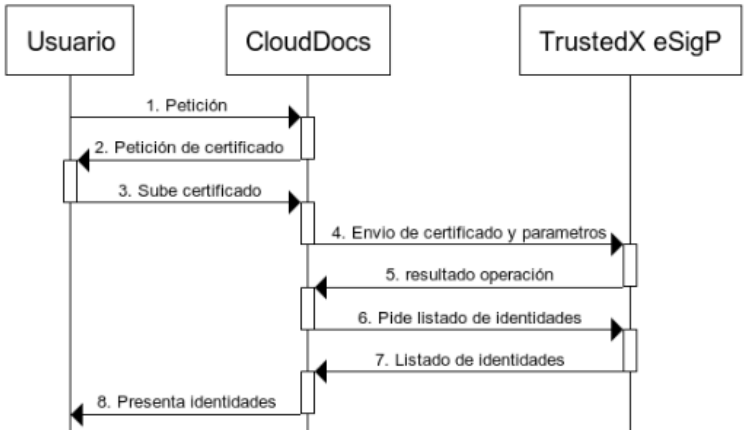


Figura 21: Caso: Agregar identidad

UC-0006	**Eliminar identidad**	
Versión	1.0	
Dependencias	[IRQ-0003] Cuenta proveedor eIDAS [OBJ-0013] Gestión de identidades	
Descripción	El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando Un usuario con cuenta en el proveedor eIDAS puede eliminar un certificado contenido en el proveedor	
Precondición	El usuario debe tener una cuenta activa	
Secuencia normal	**Paso**	**Acción**
	1	El usuario (ACT-0001) realizar una petición para eliminar una identidad
	2	CloudDocs (ACT-0002) pide la acción al Proveedor eIDAS (ACT-0003)
	3	Proveedor eIDAS (ACT-0003) responde con una aprobación
	4	CloudDocs (ACT-0002) realiza una llamada a la API del Proveedor eIDAS (ACT-0003) para obtener un listado de las identidades
	5	El proveedor eIDAS (ACT-0003) devuelve un listado de identidades
	6	CloudDocs (ACT-0002) presenta al usuario (ACT-0001) su información
Postcondición	El certificado es eliminado en la plataforma del proveedor eIDAS	
Excepciones	Ninguno	
Comentarios	Ninguno	

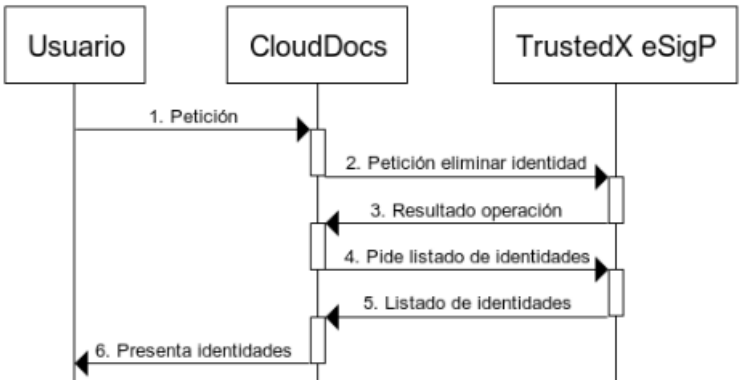


Figura 22: Caso: Eliminar identidad

UC-0007	**Firma de documentos**	
Versión	1.0	
Dependencias	[OBJ-0001] Firma digital [OBJ-0012] Gestión de identidades [OBJ-0013] Gestión de identidades	
Descripción	Un usuario con cuenta activa en el proveedor eIDAS y certificados contenidos en dicho proveedor puede realizar firma electrónica sobre un fichero PDF almacenado en un proveedor de almacenamiento.	
Precondición	El usuario debe tener una cuenta activa para el proveedor de eIDAS y proveedor de almacenamiento, así como una identidad seleccionada.	
Secuencia normal	**Paso**	**Acción**
	1	El usuario (ACT-0001) pide firmar un documento a CloudDocs (ACT-0002) para un proveedor eIDAS (ACT-0003)
	2	CloudDocs (ACT-0002) pide al usuario (ACT-0001seleccionar un proveedor eIDAS (ACT-0003)
	3	El usuario (ACT-0001) escoge el proveedor
	4	CloudDocs (ACT-0002) redirecciona al proveedor eIDAS (ACT-0003) para autorizar la firma
	5	El usuario (ACT-0001) da su consentimiento
	6	Proveedor eIDAS (ACT-0003) responde con un atributo code
	7	CloudDocs (ACT-0002) pide a Proveedor eIDAS (ACT-0003) un token en referencia al code
	8	Proveedor eIDAS (ACT-0003) recibe code y devuelve un token
	9	CloudDocs (ACT-0002) envía al Proveedor de almacenamiento (ACT-0005) la petición de descarga de fichero
	10	Proveedor de almacenamiento (ACT-0005) devuelve a CloudDocs (ACT-0002) el fichero

	11	CloudDocs (ACT-0002) particiona el fichero PDF y calcula hash
	12	CloudDocs (ACT-0002) envía hash al Proveedor eIDAS (ACT-0003) junto al identificador de la identidad
	13	Proveedor eIDAS (ACT-0003) devuelve hash firmado en formato PKCS #1
	14	CloudDocs (ACT-0002) monta la firma sobre el fichero PDF
	15	CloudDocs (ACT-0002) envía el fichero PDF firmado al Proveedor de almacenamiento (ACT-0005)
	16	Proveedor de almacenamiento (ACT-0005) respuesta satisfactoria.
	17	CloudDocs (ACT-0002) realiza una llamada a la API del Proveedor eIDAS (ACT-0003) para obtener un listado de las identidades
	18	El proveedor eIDAS (ACT-0003) devuelve un listado de identidades
	19	CloudDocs (ACT-0002) presenta al usuario (ACT-0001) su información
Postcondición		
Excepciones	**Paso**	**Acción**
	5	Si el usuario (ACT-0001) no da su consentimiento, la acción finaliza sin resultado
Comentarios	Ninguno	

Se representa una comunicación real entre CloudDocs, un proveedor de almacenamiento y los servicios que intervienen en TrustedX.

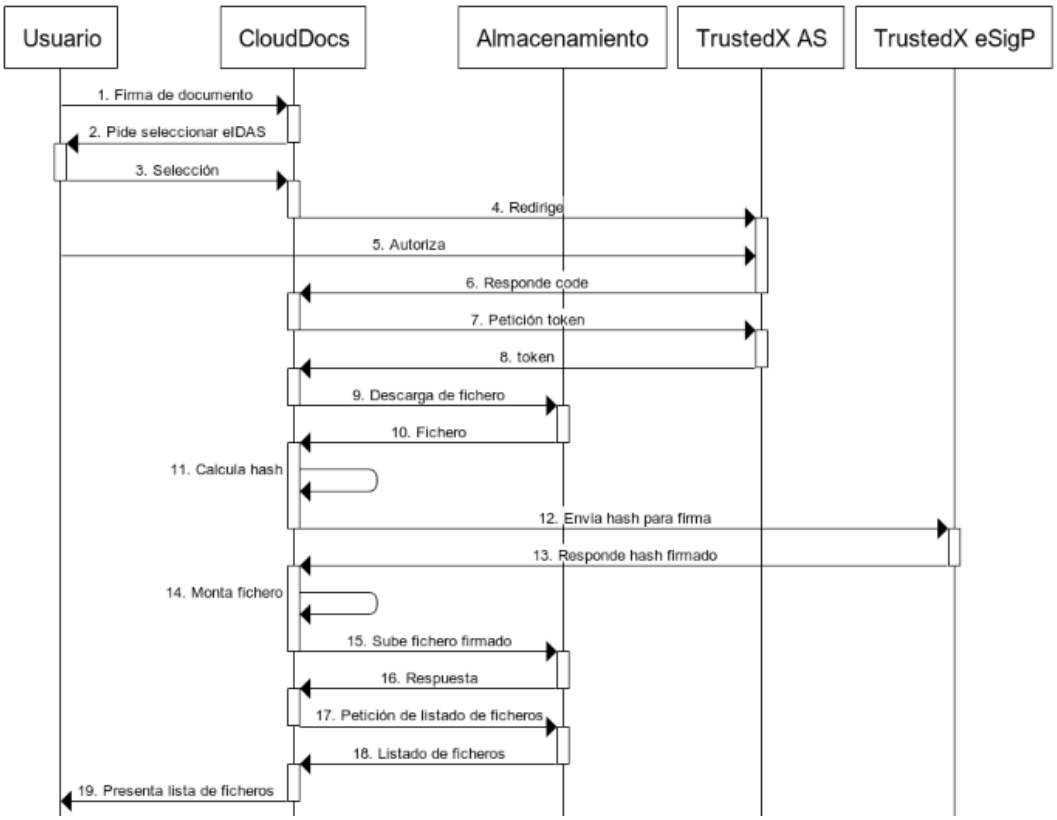


Figura 23: Caso: Firma digital

4. Implementación

La implementación de esta aplicación se lleva a cabo con el lenguaje de programación PHP versión 7 y, con ayuda del framework Slim3 se puede evolucionar a la programación orienta a objeto fácilmente.
Slim3 se puede considerar la mínima expresión de uno de los framework más famosos, Symfony. Slim3 en pocas palabras es un despachador que recibe una solicitud HTTP, invoca una rutina de devolución de llamada adecuada y devuelve una respuesta HTTP [10].

4.1. Diseño

Esta aplicación se divide en tres grandes módulos, presentados con anterioridad *Figura 2*, tales son: El usuario o usuarios, Proveedor de almacenamiento y proveedor eIDAS.

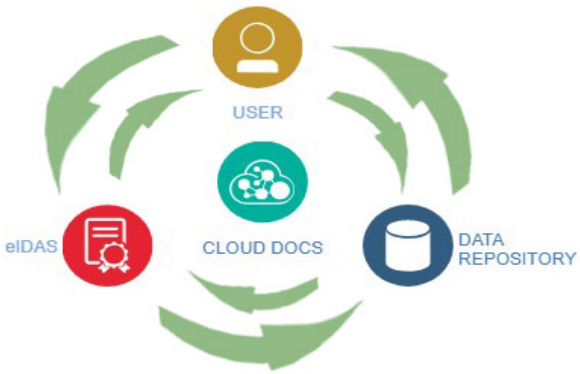


Figura 24: Módulos de implementación

El módulo de usuarios se implementa por motivos de seguridad. Este módulo da acceso a la plataforma mediante el logado de un usuario a través de un sistema o plataforma social, en nuestro caso, Google Identity.
Utilizando este medio, podemos aportar más seguridad sobre la plataforma, puesto que en ningún momento se almacena identidades ni datos personales de un individuo.

El módulo de Proveedores de almacenamiento es un componente que puede ser instanciado por uno o muchos proveedores. Este módulo gestiona las capacidades para la presentación y las firmas digital de los documentos PDF de cualquier proveedor de almacenamiento.

Para este desarrollo se va a utilizar dos de los proveedores de almacenamiento en la nube más famosos, estos son: Google Drive y Dropbox. Los cuales nos facilita su inclusión por media de la API Rest.

El módulo de Proveedores eIDAS, al igual que pasa con el módulo de Proveedores de almacenamiento, es un componente que gestiona las

capacidades para el acceso y gestión de las identidades almacenadas en el proveedor. Como peculiaridad, este módulo se encarga de la firma electrónica del fichero PDF descargado desde un proveedor de almacenamiento, es decir, se conecta a petición contra el módulo de almacenamiento.

El proveedor eIDAS que se aporta en este desarrollo es TrustedX de Safelayer. Este proveedor nos facilita su uso mediante una API Rest. Dicho proveedor dispone de diversos servicios internos como son un IdP, un servicio de autorización y eSing (servicio de identidades).

Como último modulo, se nombra a la propia plataforma que engloba al resto. Este tiene la dedicación de gestionar el correcto flujo de trabajo mediante la comprobación de rutas y acciones correctas.
Además, debe tener controlada las sesiones de los diferentes proveedores (almacenamiento y eIDAS). Esta capa estaría sobre todas las demás, almacenando todos los accesos.

A nivel técnico se encarga de la gestión las sesiones y controlador de todos los tokens.

4.2. Diseño de arquitectura

En este apartado se describe las relaciones de los diferentes elementos que intervienen en el desarrollo.

4.2.1. Presentación

La capa de presentación entrega a un usuario de la red el diseño programado para su visualización y por el cual interactúa con la aplicación.

- Pantalla de login: En esta pantalla se presenta como paso previo a entrar en la aplicación. El usuario podrá logarse con a través de un usuario Google de que disponga.
  En este modelado solo se incluye el botón de login el cual redirige al usuario a la Google Identity.

- Portal: En esta pantalla se muestra varios apartados que se procede a explicar.

    - Menu: En este parte se visualiza las diferentes opciones que tiene el usuario para navegar por la aplicación.

    - Contenido: Este contenido varía según la opción del menú escogida.

        - Apartado Inicio: se muestra un contenido con una descripción simple del proceso de firma digital para un documento pdf.

- Apartado Perfil: con los datos recogidos del usuario logado sobre Google, se lanza una plantilla donde el propio usuario puede ver sus datos como son Nombre, Apellidos, Email y la foto de perfil actual.

- Apartado eIDAS: Cuando un usuario aún no se ha logado contra el proveedor eIDAS, en este caso TrustedX, muestra un link para que el usuario sea redirigido a su servicio IdP.

  Cuando el usuario se ha logado el contenido que muestra es una lista de las identidades del usuario

- Apartado Ficheros: En este caso, puesto que hay dos proveedores de almacenamiento, se presentan dos opciones que muestran la misma plantilla.
  Si el usuario aún no se ha logado sobre el proveedor de almacenamiento, muestra un link para ser redirigido a su IdP.
  Si el usuario ya está logado, se muestra una lista de ficheros PDF que almacena el proveedor de ficheros para el usuario.

4.2.2. Modelo de datos

El desarrollo de esta aplicación se realiza en base al modelo MVC (Modelo-vista-controlador), se detalla a continuación cada apartado.

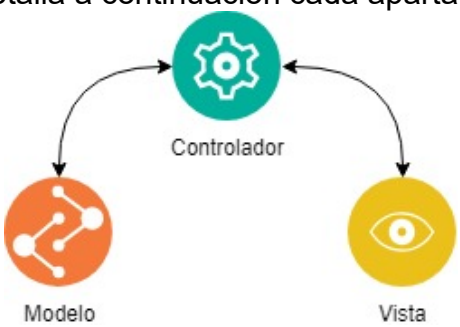


Figura 25: MVC

4.2.2.1. Controladores

Se desarrolla un controlador por cada capa de presentación. Estos actuadores toman el control lógico de las entradas ejecutadas por el usuario, es decir, realiza las funciones que pide un usuario.

Los controladores son los siguientes:

- Inicio: Es un controlador simple que muestra instrucciones al usuario para la firma digital de un documento.

- Login: Maneja los diferente token y datos necesarios para mantener al usuario logado en la plataforma.

  Este controlador maneja la siguiente lista de variables bajo la sesión de un usuario:

Variable	Descripción
#token_id	token de google Oauth2
#googledrive	token referente al acceso a fichero google
#dropbox	token referente al acceso a dropbox
#trustedx_oauth	token referente al acceso de un usuario a TrustedX (Safelayer)
#state	state para comprobar la verificación de la petición a TrustedX (Safelayer)
#id_user_trustedx	id del usuario trustedX
#sign_trustedx	identificador de la firma para la posterior firma digital
#id	id del usuario registrado por Google
#email	email del usuario logado por Google
#is_logged	Si esta logado el usuario (variable boolean)
#type	Especifica el tipo de usuario que se ha logado. En este desarrollo siempre marcara “Google”

  Este controlador tiene la clase LoginAction

- Login Google: Este actuador presta el servicio para la comunicación contra Google Identity y poder así realizar un logado correcto del usuario.

  Este controlador tiene la clase OAuth2GoogleAction

- Proveedor de almacenamiento: Controla la comunicación de logado de un usuario para cada una de las dos plataformas de almacenamiento existente. Así pues, también controla la descarga de ficheros formateando las cabeceras.

  Este controlador tiene las clases DropboxFileAction y GoogleFileAction.

- Proveedor eIDAS: Controla las acciones de logado de un usuario contra el servicio de TrustedX, la carga y eliminación de identidades y la firma de ficheros PDF.

  Este controlador tiene la clase TrustedXAction

4.2.2.2. Modelos

Se detalla cada uno de los modelos construidos para dar soporte a los controladores explicados.

- Login Google: Para la correcta interpretación de la comunicación contra Google se importa una librería desarrolladas por Google (“google-api-php-client”) para trabajar con la librería desarrollada que simplifica el flujo.
  Aquí encontramos la clase “GoogleLíbrary“.

- Proveedor de almacenamiento: Se ha generado una interfaz común para todos los proveedores. Los dos proveedores que están implantados deben obedecer los métodos que la interfaz propone.

- Proveedor eIDAS: Este modelo también se ha generado una interfaz común. Aunque en el apartado de actuadores se marca al proveedor eIDAS como responsable de la firma, a nivel de modelado, la clase dedicada a TrustedX solo se definen métodos para la comunicación contra los servicios de este. A continuación, se detalla la clase que realiza la firma de un documento.

- Firma: Esta librería se encarga exclusivamente de la firma de un documento PDF.
  Se debe tener en cuenta que el usuario solo da su consentimiento a la aplicación Cloud Docs para trabajar con los ficheros, por tanto, no se suministra ningún fichero a terceros proveedores. Con esto se quiere decir, que es el propio portal quien firma el documento con ayuda de un proveedor eIDAS.
  Aquí se trabaja con todas los demás modelos. Se utiliza el proveedor de almacenamiento para la descarga del documento PDF y el proveedor eIDAS para la firma de hash que realiza esta clase.
  Esta clase utiliza una librería a más bajo nivel, llamada SetaPDF con la cual se trabaja con licencia temporal. Esta librería nos permite realizar una firma asimétrica PAdES (aprobado por el marco eIDAS) e incluso incluir detalles como sellado del documento y la incorporación de fecha y hora haciendo uso de un TSP (Time-Stamp Protocol) según a la RFC 3161.

4.2.2.3. Vistas

Para el conjunto de vistas se utiliza twig, una extensión famosa utilizada por Symfony. Este nos permite heredar vistas para realizar un conjunto. Se configura de tal forma:

- Vista Error: En esta vista se muestran algún error que no haya sido controlado por los diferente modulos.

- Vista login: Se presente una interfaz con solo el botón de Acceso con Google.

- Vista home: Una interfaz con información básica de cómo proceder con una firma digital.

- Vista Proveedor de almacenamiento: esta vista hereda hacia las dos interfaces de Google y Dropbox. Aunque en ambas se carga la misma estructura de datos, se considera que puede ser más fácil desarrollar.

- Vista de Proveedores eIDAS: También se lleva a cabo un modelo de herencia. En este caso se presente solo una interfaz de TrustedX, dicha interfaz conglomera toda la información en una misma pantalla, de tal modo no hace necesario pasar por más vista.

  En esta misma vista se hace uso de jquery para poder introducir la contraseña de una identidad a subir.

4.2.3. Aplicaciones utilizadas

A continuación, se presentan las tecnologías utilizadas para el desarrollo de este proyecto y aplicaciones de ayuda.

Tecnología	Descripción
PHP	Lenguaje de programación del lado del servidor.
	URL: https://secure.php.net/
Apache	Servidor web HTTP
	URL: https://apache.org
Slim 3	Microframework PHP simple para desarrollo de aplicaciones y API
	URL: https://www.slimframework.com/
Twig	Lenguajes de plantilla basados en texto
	URL: https://www.slimframework.com/
BootTrap	Plantillas de diseño para múltiples elementos.
	URL: https://getbootstrap.com

Bootstrap Magic 4.0	Constructor de plantillas con base boottrap.
	URL: https://pikock.github.io/bootstrap-magic/
Jquery	Librería javascript utilizado para la extensiçon jquery-confirm
	URL: https://jquery.com **URL:** https://craftpip.github.io/jquery-confirm/
Decoder ASN.1	Decodificador de formato DER o VER a estructura ASN.1
	URL: https://lapo.it/asn1js/
Draw.io	Software para el desarrollo de diagramas.
	URL: https://www.draw.io/
ArgoUML	Editor de modelado UML
	URL: http://argouml.tigris.org/
PhpStorm	Editor de código para framework PHP, javascript y CSS
	URL: https://www.jetbrains.com/phpstorm/
Git	Software de control de versiones
	URL: https://bitbucket.org/
Docker	Software de automatización de despliegues en contenedores sobre una capa abstracta de virtualización.
	URL: https://www.docker.com

5. Flujo funcional

En este apartado se realiza una demostración funcional de la aplicación desde el inicio hasta la firma satisfactoria de un documento pdf.

El acceso se realiza mediante la url https://uoc.safelayer.com:9000/login que muestra la pantalla de bienvenida. El acceso a la plataforma se realiza llamando al IdP de Google por protocolo OpenID, mediante el cual permite autentica y autoriza a un usuario Google.

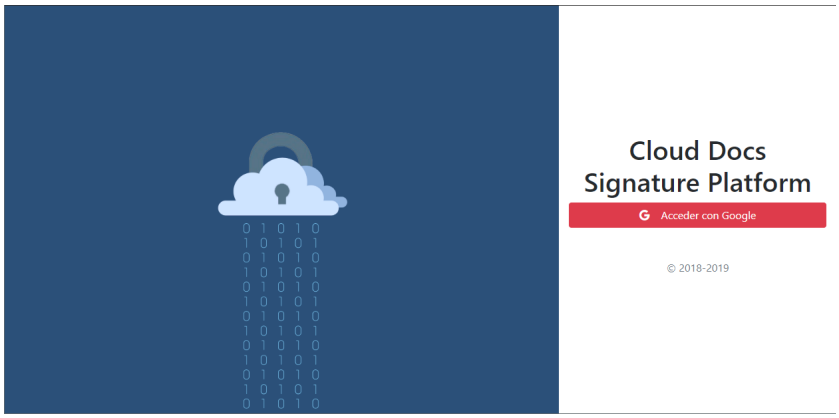


Figura 26: Pantalla inicio

En esta acción, la aplicación redirige al usuario al servidor de IdP de Google donde debe introducir una dirección de correo y contraseña para posteriormente volver a Cloud Docs Platform.

En este punto la aplicación obtiene un token de autorización con un tiempo de expiración determinado.
Con este token, la aplicación obtiene los datos deseados de la cuenta Google, sin necesidad de volver a autorizar a un usuario.

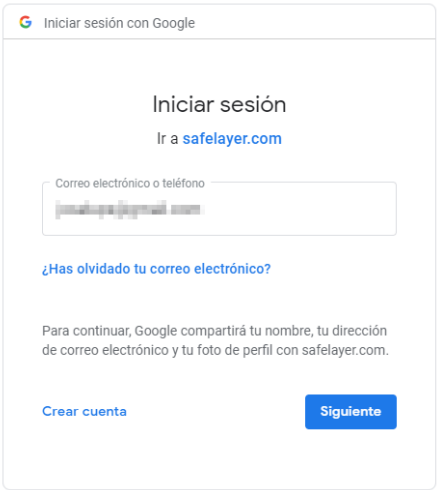


Figura 27: Inicio de sesión con Google

Tras esta acción se accede a la pantalla de perfil del usuario, donde se muestra algunos datos básicos del usuario logado, como es su nombre y dirección de correo, así como, la imagen de perfil que tenga definida.

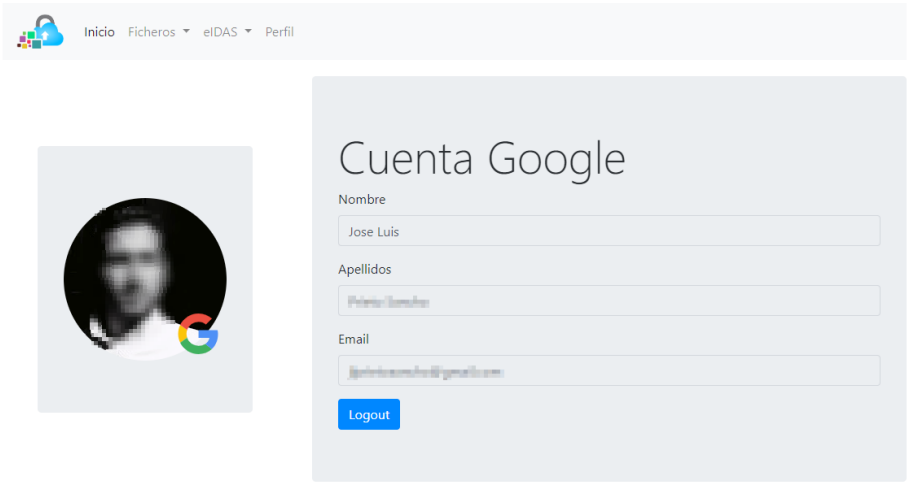


Figura 28: Pantalla de perfil

Siguiendo el flujo, el siguiente paso sería logar a un usuario en la sesión de eIDAS > TrustedX, donde nos dará la posibilidad de gestionar la identidad del usuario.

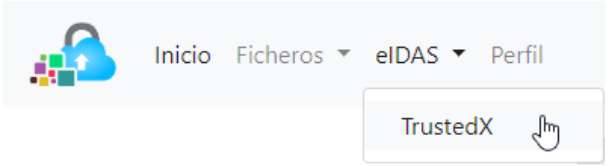
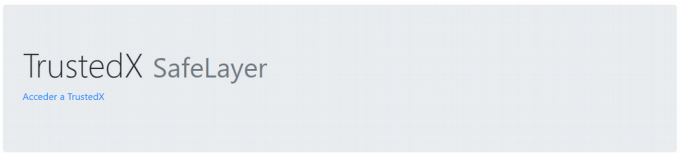


Figura 29: Menú eIDAS



Picar sobre Acceder a TrustedX, cuya acción nos conducirá al servidor IdP de TrustedX.

Figura 30: Acceso a TrustedX

El servidor nos pedirá una cuenta existente para autenticar y seguidamente autorizar al usuario.

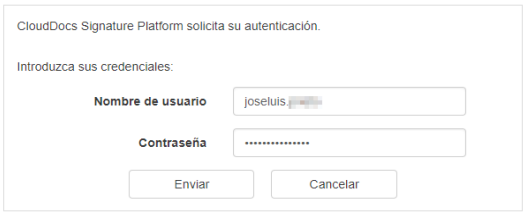
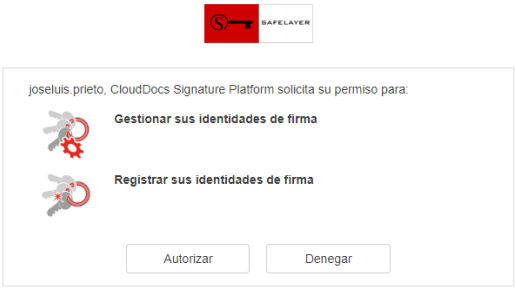


Figura 31: Inicio de sesión a TrustedX



Ahora se debe Autorizar los siguientes permisos que la aplicación requiere para gestionar la identidad/es.

Figura 32: Autorización de permisos TrustedX

La pantalla siguiente muestra campos vacíos puesto que aún no hay identidad subida al servidor HSM de eSigP.

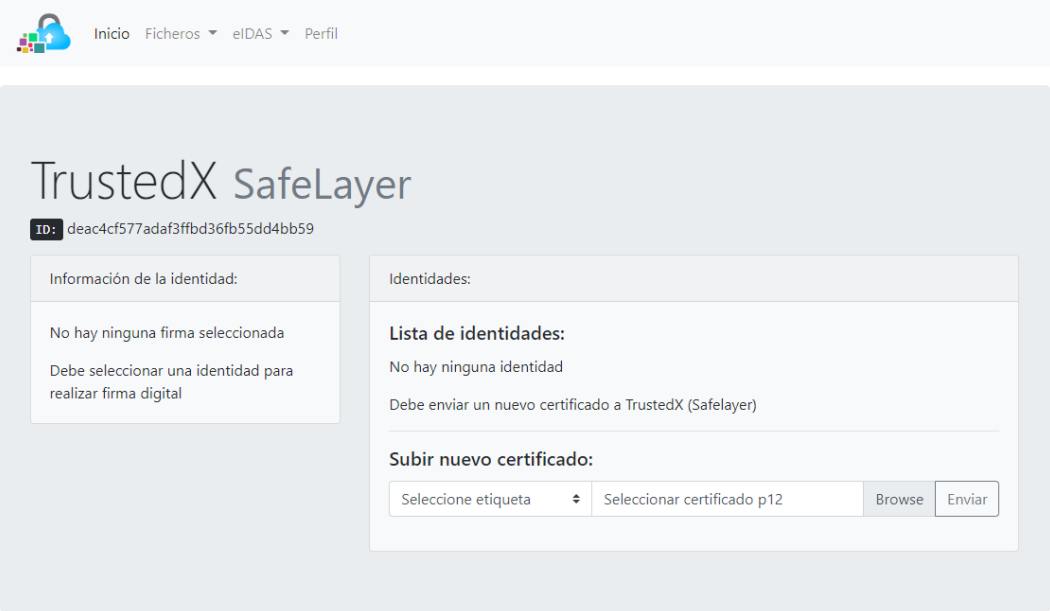


Figura 33: Pantalla inicio de TrustedX

Por tanto, se sube un certificado otorgado por la empresa SafeLayer con la identidad del usuario. Y para ello se debe seleccionar una etiqueta entre las disponibles, seleccionar el certificado mediante un brower explorer.

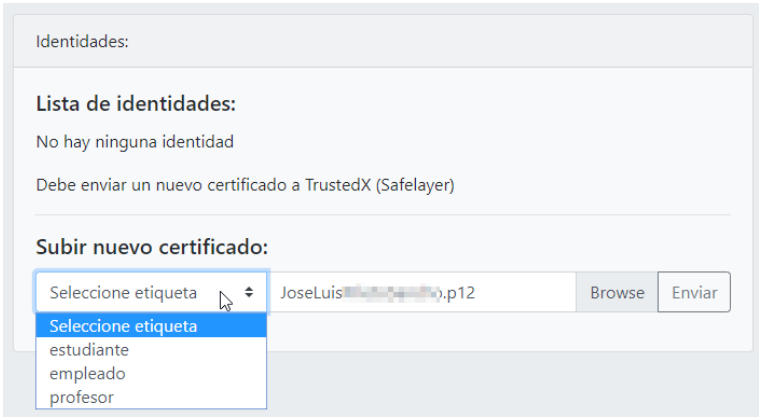


Figura 34: Subir identidad a TrustedX

Al pulsar sobre el botón enviar pedirá la contraseña para el certificado. p12 que se ha adjuntado.

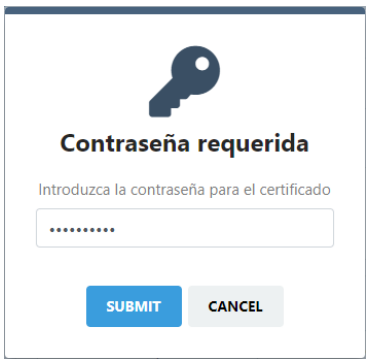


Figura 35: Contraseña para identidad

Si el certificado y la contraseña son correctas la identidad queda registrada en el servidor de eSigP de TrustedX y aparecerá en el apartado de identidades la identidad subida.
Si se requiere, se puede subir cuantas identidades se desee, para después trabajar con ellas.

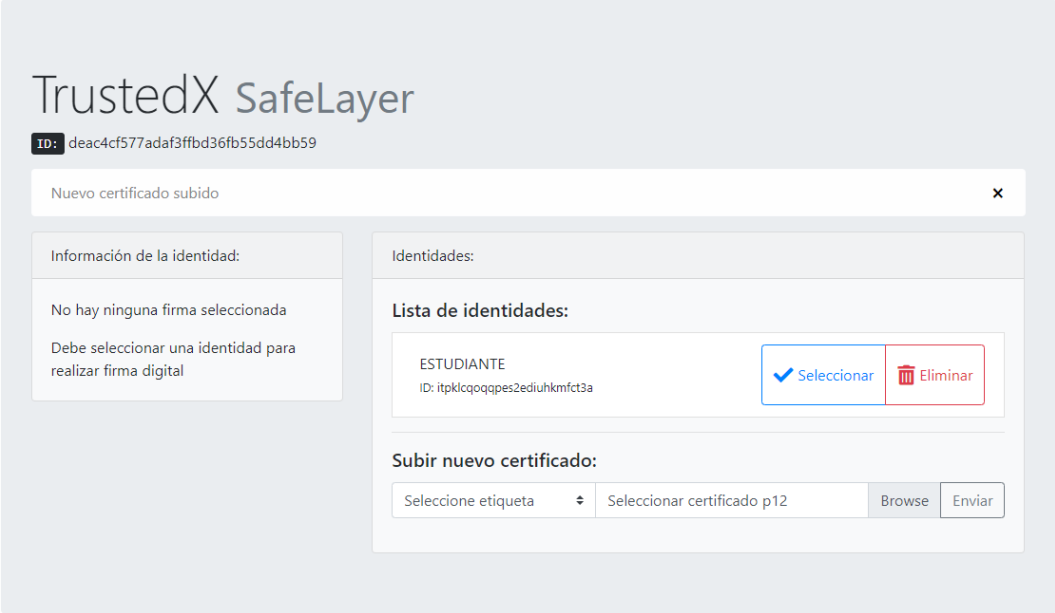


Figura 36: Nueva identidad subida

Siguiente paso, se debe seleccionar una de las identidades para posteriormente realizar la firma sobre los documentos PDF que se desee.

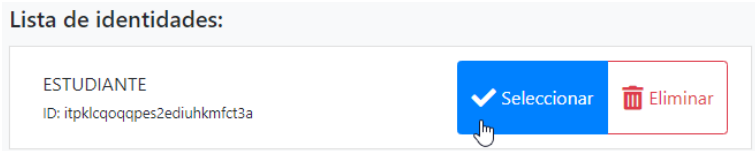


Figura 37: Selección de identidad

Con esta acción, hace que en el apartado de Información de la identidad aparezca los detalles de la identidad seleccionada.

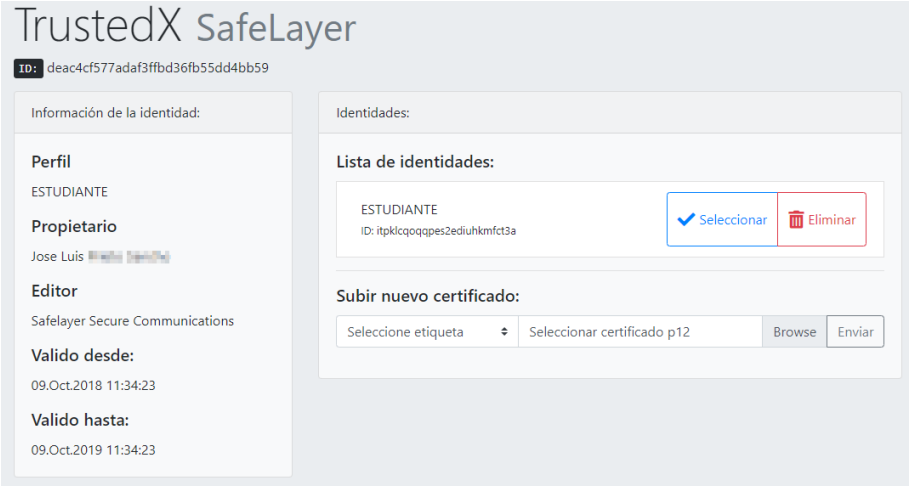


Figura 38: Pantalla con identidad seleccionada

A continuación, se debe ir al apartado del menú, Ficheros, donde se puede optar por dos proveedores de almacenamientos.

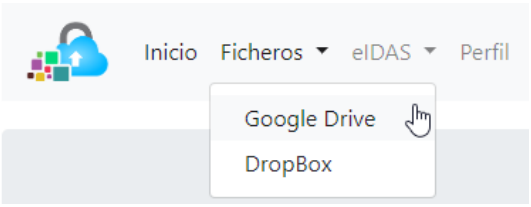


Figura 39: Menú Ficheros

Para el apartado de ficheros Google Drive aparecerá la siguiente pantalla donde se debe picar sobre Acceso a Google Drive para Autenticar y Autorizar al usuario a acceder a su contenido.

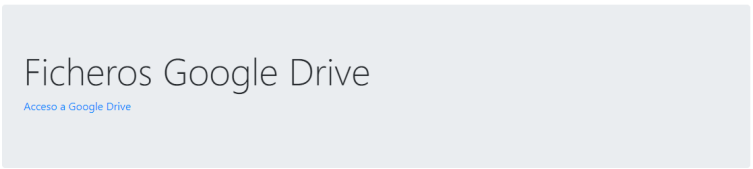
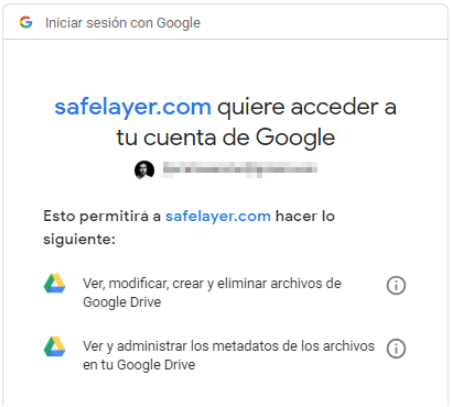


Figura 40: Acceso a Google Drive



Esta acción vuelve a redirigir al usuario al servidor IdP de Google, donde debe seleccionar una cuenta y autorizar los permisos.

En el caso que solo exista autenticada en el navegador (cookie Google.com) solo la cuenta con la que se accede a la aplicación, el usuario será redirigido directamente a la pantalla de autorización.

Figura 41: Autorización de permisos para Google Drive

Para el apartado de fichero DropBox aparecerá la siguiente pantalla donde se debe picar sobre el enlace Acceso a Dropbox.

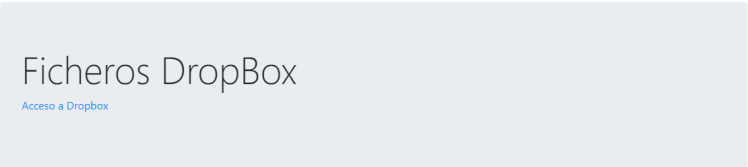


Figura 42: Acceso a DropBox

Siguiendo la misma dinámica, el usuario será redirigido a Dropbox para autenticar a un usuario y autorizar el acceso a la aplicación CloudDocs.

Figura 43: Autenticación a DropBox

Una vez autenticado en alguno o los dos proveedores de almacenamiento se presentan un listado de documento PDF.
Ahora, el siguiente paso es proceder al firmado de un documento PDF con la identidad seleccionada anteriormente. Para ello elegimos el documento y pulsamos sobre el botón Firmar.

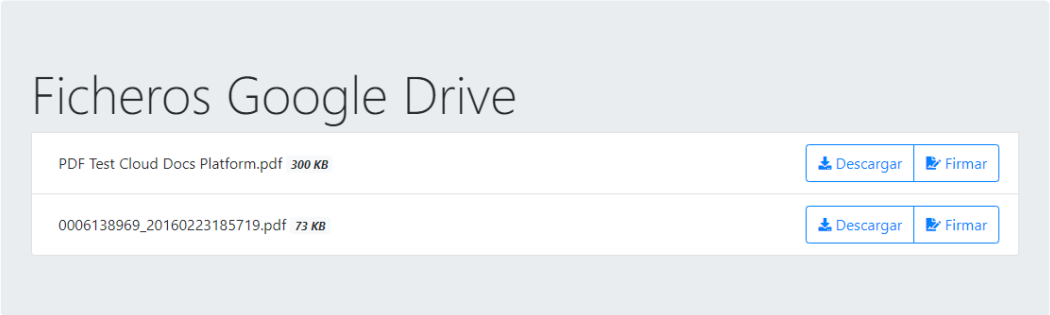


Figura 44: Listado de ficheros Google Drive

En ese momento pedirá con que proveedor desea firmar. Se pulsar sobre TRUSTEDX.

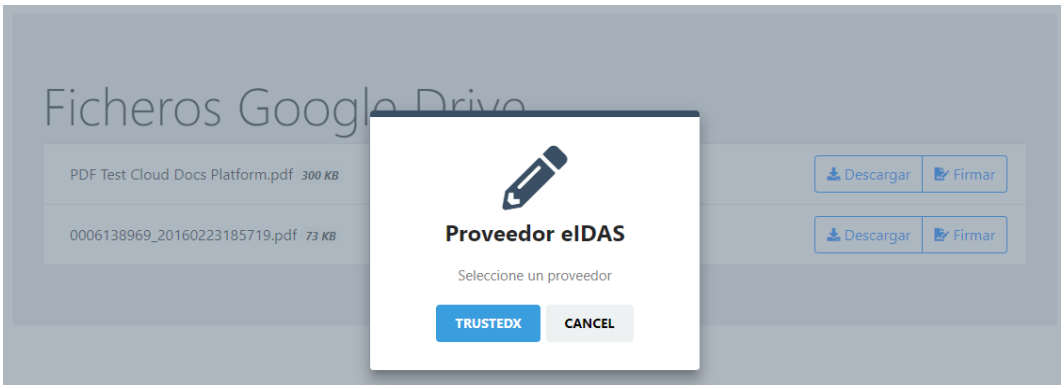


Figura 45: Selección de identidad

A continuación, la aplicación redirige al usuario al servidor AS de TrustedX para autorizar el permiso de firma.

Si es autoriza, la aplicación procede a la descarga del documento, firma de tal y por último sube el documento al proveedor de almacenamiento.

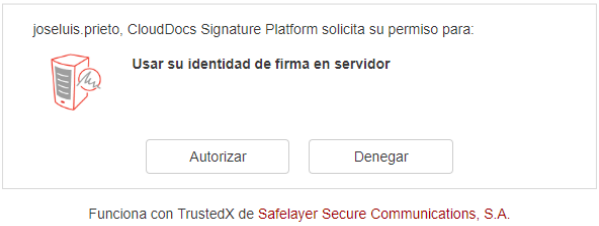


Figura 46: Autorización de firma para TrustedX

Una vez finalizada la acción se presenta el listado de ficheros con el nuevo documento firmado. Dicho documento tiene una terminación como *-cloudDoc-sign.pdf

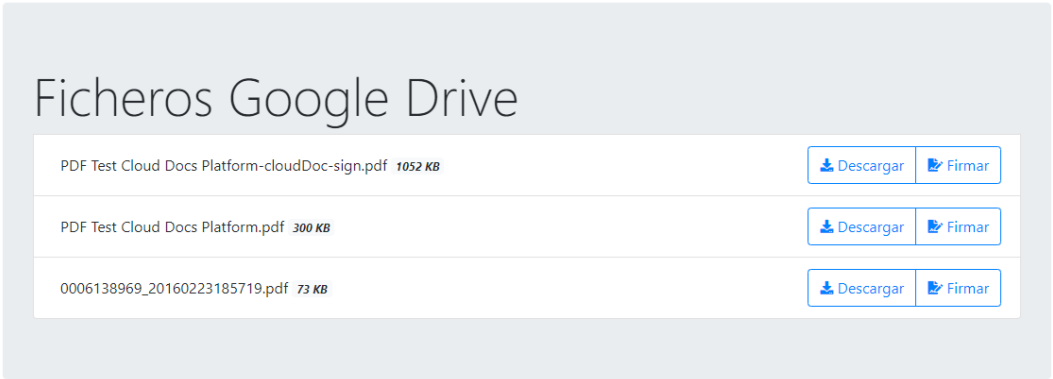


Figura 47: Listado ficheros Google Drive

Para obtener el documento se pica sobre el botón Descargar del documento firmado.

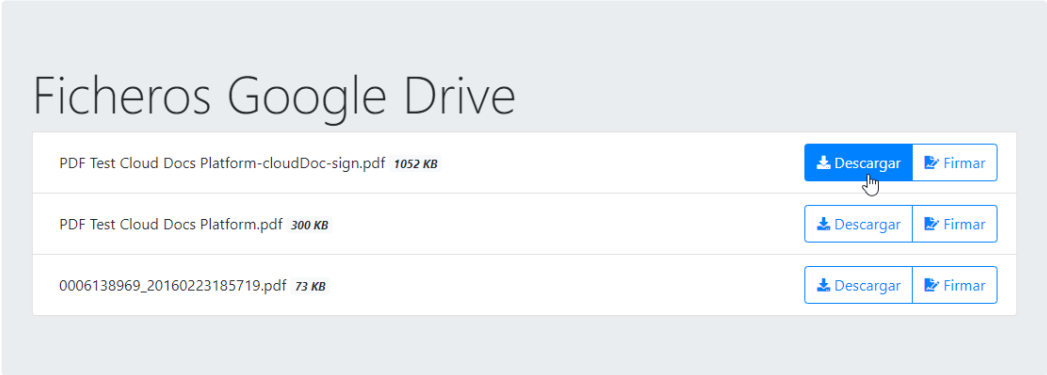


Figura 48: Descarga de fichero firmado

Para comprobar la autenticidad del documento se puede abrir con el software Adobe Acrobat Reader.

Se puede desplegar el menú de Firmas para visualizar los campos de la firma.

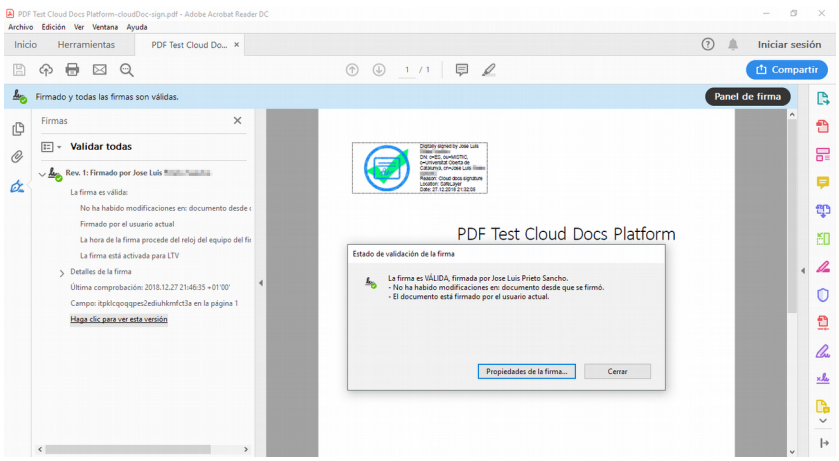


Figura 49: PDF firmado

También se puede ver el certificado del firmante.

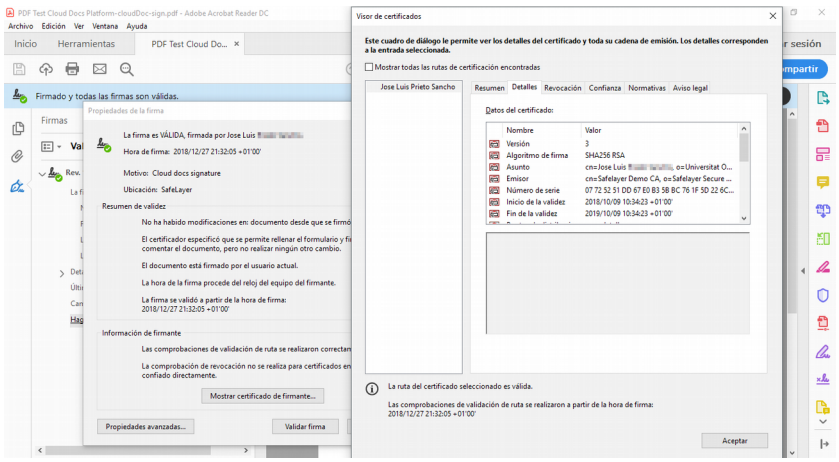


Figura 50: Certificado contenido en un PDF

6. Conclusiones

Gracias al alcance de este proyecto se hace presente una unificación electrónica a nivel europeo. Esta unificación viene dada por el Reglamento eIDAS por el cual se abre nuevos caminos de comunicación segura.
La aplicación desarrollada presenta una intersección entre seguridad de usuario, firma electrónica y gestión de la identidad electrónica sobre un servicio de confianza. Y para este caso se confía en la empresa SafeLayer con su producto TrustedX que nos facilita la interacción por medio de su API REST.

Esta aplicación guarda en todo momento la privacidad, puesto que no se almacena registro de actividad del usuario. Haciendo uso de los diferentes protocolos estudiados se puede realizar un flujo de trabajo, para la firma electrónica, sin necesidad de tener retener datos de usuarios.

A vista futura, se tomó la decisión de dejar un desarrollo abierto para una posible expansión de servicios, tanto para la parte de almacenamiento como para la parte de servicios de confianza eIDAS.
Unos de los servicios de almacenamiento que puede ser de interés, el cual por tiempo no se ha podido implantar, es WeTransfer (un servicio donde la documentación es volátil).
Para el caso del servicio eIDAS, puesto que se ha trabajado contra una demo sería un acierto poder adecuarlo a un servicio productivo y ofrecer así una firma cualificada.

El desarrollo se ha realizado con un lenguaje de programación versátil y muy conocido por programadores. También se han utilizados numerosas librerías que han ayudado a vitaminar la estructura de front-end.
Para trabajar con este lenguaje ha hecho falta realizar una preinstalación de productos virtuales para la presentación de contenido web, así como la instalación de librerías técnicas que han ayudado al correcto funcionamiento de determinadas acciones de la aplicación.
En la fase de puesta en producción se ha decido realizar una plantilla de despliegue para Docker. Así el encapsulado, en este caso contenedor, puede desplegarse en pocos minutos. También se ha descrito instrucciones de instalación para un sistema Linux en el manual de despliegue.

Por concluir, como hito personal me ha supuesto un gran reto e interés el estudio del reglamento eIDAS utilizado, el desarrollo de la comunicación mediante API REST a los diferentes servicios y la firma electrónica asíncrona sobre documentos PDF, donde se pudo observar toda la estructura de seguridad que ofrece la versión PDF 1.7.

7. Glosario

GANTT: Herramienta que expone la dedicación en tiempo de cada tarea programada.

eIDAS: electronic IDentification, Authentication and trust Services o sistema europeo de reconocimiento de identidades electrónicas es un Reglamento Europeo que conforma un marco normativo para la identidad electrónica.

Oauth 2.0: Protocolo de autorización segura.

OpenID: Protocolo de autenticación segura de la familia de especificaciones Oauth2.0.

SAML 2.0: Estándar de intercambio de datos para autenticación y autorización entre dominios de confianza, es decir entre un proveedor de identidad y un consumidor.

SSO: Single Sign-On, sistema de autenticación unitaria que permite el acceso a varios sistemas con una sola autenticación.

API REST: Arquitectura con estándar HTTP que puede ser utilizado por cualquier aplicación.

IdP: Proveedor de identidad, sistema de confianza que confirma la identidad de un usuario.

AS: Servidor de autenticación, servicio dedicado para la autenticación de credenciales.

HSM: Hardware Security Module, módulos que ayudan al cifrado de datos, generación de claves y almacenamiento de contraseñas.

eSigP: Proveedor de firma electrónica, servicio de confianza que permite elevar el factor de autenticación (según eIDAS Assurance Levels)

PAdES: Es un conjunto de restricciones y extensiones adecuado para la firma electrónica avanzada.

8. Bibliografía

[1] «Globalización» [En línea]. Available: https://es.wikipedia.org/wiki/Globalizaci%C3%B3n

[2] M. d. e. y. e., «Servicios electrónicos de confianza,» [En línea]. Available: https://www.mincotur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/preguntas-frecuentes.aspx

[3] «OAuth 2.0,» [En línea]. Available: https://oauth.net/2/

[4] «Google Identity Platform,» [En línea]. Available: https://developers.google.com/identity/

[5] «Service Providers,» [En línea]. Available: https://www2.empowerid.com/learningcenter/technologies/service-identity-providers

[6] «OpenID,» [En línea]. Available: https://es.wikipedia.org/wiki/OpenID

[7] «Protocolo Oauth2,» [En línea]. Available: https://es.wikipedia.org/wiki/OAuth

[8] «Api Google Drive,» [En línea]. Available: https://developers.google.com/drive/api/v3/about-auth

[9] «Framework Slim 3,» [En línea]. Available: https://www.slimframework.com/docs/

[10] «Concept of SAML, OAuth2 and OpenID Connect,» [En línea]. Available: http://www.resilient-networks.com/concept-week-saml-oauth2-openid-connect/

[11] «Electronic Signatures and Infrastructures,» [En línea]. Available: https://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf.

[12] «PDF 32000-1,» [En línea]. Available: https://www.adobe.com/content/dam/acom/en/devnet/acrobat/pdfs/PDF32000_2008.pdf.

[13] «SetaPDF-Signer» [En línea]. Available: https://manuals.setasign.com/setapdf-signer-manual/.

[14] «PAdES» [En línea]. Available: https://www.viafirma.com/es/pades-firma-electronica-avanzada-en-formato-pdf.

[15] «Trustedx eidas platform» [En línea]. Available: https://www.safelayer.com/es/productos/trustedx-eidas-platform.

9. Anexos

- Manual de usuario: Documento explicativo de la funcionalidad de la aplicación para el usuario consumidor.

- Documento de despliegue: Documento explicativo para la implantación de la aplicación mediante Docker o en sistemas Linux.

- Repositorio CloudDocs: Repositorio de código de la aplicación
  URL: https://bitbucket.org/josprisan/clouddocs/src/master/

- Repositorio Docker: Repositorio con los ficheros necesarios para el despliegue de una imagen mediante Docker.
  URL: https://bitbucket.org/josprisan/docker/src/master/

- Docker: imagen preconstruida de Docker
  URL: https://cloud.docker.com/repo/docker/josprisan/clouddocs/