CloudDocs Signature Platform

Albert Forns Verge
Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions

Consultor: Juan Carlos Fernández Jara
Centre: Universitat Oberta de Catalunya

Data lliurament: 02/06/2018

AGRAÏMENTS

En primer lloc vull agrair al Juan Carlos l'interès mostrat des de l'inici d'aquest TFM i per guiar-me durant les diferents fases del projecte per tal de poder assolir els objectius marcats.

Però sobretot, voldria donar les gràcies a la Tatiana pel suport que m'ha donat durant aquests anys que he cursat el màster i la paciència que ha tingut.

Títol del treball:	CloudDocs Signature Platform
Nom de l'autor:	Albert Forns Verge
Nom del consultor/a:	Juan Carlos Fernández Jara
Nom del PRA:	Juan Carlos Fernández Jara
Data de lliurament (mm/aaaa):	06/2018
Titulació o programa:	Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)
Àrea del Treball Final:	TFM – Ad hoc
Idioma del treball:	Català
Paraules clau	cloud signatura

Resum del treball

Els canvis normatius introduïts en Reglament Europeu 910/201, conegut com eIDAS, han eliminat restriccions en la realització de signatures qualificades i han permès l'aparició de serveis de signatura al cloud.
L'objectiu d'aquest TFM és fer ús d'aquests serveis juntament amb serveis d'emmagatzematge en el cloud, molt estesos entre els usuaris, per tal de poder realitzar signatures qualificades de documents PDF allotjats en aquests serveis d'una forma senzilla pels usuaris que no requereixi instal·lacions.

Abstract

The regulatory changes introduced in European Regulation 910/201, known as eIDAS, have eliminated restrictions on the production of qualified signatures and have allowed the emergence of cloud signing services.
The aim of this TFM is to use these services along with cloud storage services, which are widely used among users, in order to be able to make qualified signatures of PDF documents hosted in these file storege services in an easy way for them and that do not require installations.

Índex

Llista de figures

1. Introducció

1.1. Context i justificació del Treball

La legislació actual a través del Reglament Europeu 910/2014 [1] conegut com eIDAS busca potenciar els serveis d'identificació i firma electrònica. Estableix les condicions en què els estats membres hauran de reconèixer els mitjans d'identificació electrònica de les persones físiques i jurídiques que pertanyin a un sistema d'identificació electrònica notificat d'un altre estat membre, al mateix temps que estableix unes regles pels serveis de confiança per les transaccions electròniques i es crea un marc jurídic per la signatura electrònica, segells i marques de temps, documents electrònics així com els serveis d'entrega registrada (correu electrònic certificat) i serveis de de certificats per l'autenticació en llocs web. Un dels principals canvis doncs, és que una firma electrònica qualificada serà reconeguda en tots els estats membres, independentment de l'estat en que s'hagi realitzat. [2]

Per tal de poder d'estimular l'ús dels serveis descrits anteriorment cal facilitar als ciutadans unes eines que resultin còmodes i no siguin complexes d'utilitzar. Actualment milions de persones utilitzen serveis al núvol per a emmagatzemar documents personals o laborals degut a la comoditat, seguretat i altres avantatges que aquests ofereixen. Aquestes plataformes permeten accedir als propis fitxers des de qualsevol dispositiu amb internet des de qualsevol part del món, no requereixen cap tipus d'instal·lació de software ja que tot es realitza via web, són eines intuïtives i senzilles d'utilitzar, permet compartir els documents amb altres usuaris i, fins i tot permet que varis usuaris treballin simultàniament amb el mateix document, accepta que es pugui treballar sense connexió a la xarxa i sincronitzar els documents posteriorment.

Els serveis al núvol (cloud services) són serveis que es posen a disposició sota demanda dels usuaris a través d'Internet enlloc de proporciona-ho als servidors locals d'una empresa. Molts d'aquests serveis es contracten a través de subscripcions on es paga una quota mentre se'n fa ús, i un cop no és necessari es dona de baixa. Això permet a les empreses disposar de programari, emmagatzematge i altres elements d'infraestructura sense haver de fer grans inversions inicials, ni haver de disposar d'un equip especialitzat per a fer les instal·lacions i manteniments.
Aquests serveis estan dissenyats per proporcionar un accés fàcil i escalable a recursos, els quals poden ser de programari (SaaS: Software-as-a-Service), infraestructura (IaaS: Infrastructure-as-a-Service), plataforma (PaaS: Platform-as-a-Service), etc..
La plataforma Google Drive és un exemple de serveis al núvol que ofereix al mateix temps IaaS per a l'emmagatzematge de fitxers i SaaS per al programari de creació de documents

Un certificat digital és un document digital mitjançant el qual, un tercer de confiança, una autoritat de certificació, garanteix la vinculació entre la identitat d'un subjecte o entitat i la seva clau pública. Un dels usos d'un certificat digital és la realització de signatures electròniques de documents. En els reglaments anteriors, ja sigui a nivell nacional (Llei de Firma Electrònica 59/2003 de 19 de desembre [3]) com a nivell europeu (Directiva Europea 1999/93/CE de desembre del 1999 [4]), la realització d'una signatura electrònica qualificada era més restrictiva ja que requeria un dispositiu segur de creació de signatura com podria ser una targeta criptogràfica. Amb l'entrada en vigor de la nova normativa, es modifica la definició d'allò que és un dispositiu qualificat de creació de signatura / segell electrònic; aquests han de complir els requisits llistats a l'annex II del Reglament Europeu 910/2014 [1]. Es poden realitzar signatures electròniques qualificades amb dispositius de creació de signatura, que tot i estar sota

el control del signant, es pot ubicar en dispositius que no siguin hardware, per exemple, software o inclús al núvol.
Aquest canvi normatiu permet la implementació d'un nou tipus servei al núvol on els recursos d'aquests són els certificats digitals i ofereixen realitzar operacions amb aquests. Fabricants de software com Safelayer aprofiten aquest fet per oferir un dispositiu qualificat de creació de signatures enfocat als serveis al núvol. Els seus usuaris poden accedir i consumir els seus serveis de signatura electrònica de la mateixa forma que s'utilitzen plataformes com Google Drive.

L'ús dels certificats digitals per a realitzar la signatura electrònica qualificada [5] pot comportar una sèrie de problemes o inconvenients als usuaris que podem intentar minimitzar per tal que l'experiència d'usuari sigui més senzilla i còmoda. A més, també és necessari tenir instal·lat un software específic per a poder realitzar la signatura, ja sigui a través d'aplicacions com podrien ser Adobe Acrobat Reader, applets de Java (tot i que el seu ús ja està obsolet i s'està substituint per Java Web Start [6]), etc... Aquestes aplicacions requereixen que els certificats que es vulguin utilitzar estiguin instal·lats en local al dispositiu on s'estiguin executant, fet que no facilita la mobilitat o l'ús d'aquests en diversos dispositius. Una possible solució per a mitigar aquest punt són els serveis de signatura avançada qualificada que ens permeten emprar les nostres claus des de qualsevol dispositiu sense necessitat d'instal·lació. En aquest punt és on apareixen serveis de signatura, com és el cas de TrustedX utilitzat en aquest TFM, que permeten realitzar la signatura qualificada al cloud.

Aquest projecte pretén integrar dos ecosistemes del núvol amb la mateixa filosofia: servidors de recursos que interaccionen sempre sota el control exclusiu de l'usuari garantint en tot moment la seguretat d'accés i us d'aquests recursos, tal com es veurà al treball. Per un costat, tindrem els servidors de recursos d'emmagatzematge de fitxers i per altre costat, els servidors de recursos d'identitats que ens permetran realitzar signatures electròniques qualificades dels fitxers ubicats al núvol.

Aquesta plataforma té com a objectiu facilitar als usuaris la realització de signatura qualificada de documents PDF ubicats al cloud utilitzant únicament un navegador web sense requerir cap software afegit i complint amb la normativa actual. Per tal de dur a terme aquestes idees, s'ha implementat una aplicació web des de zero que incorpora totes les peces necessàries mínimes per a complir els objectius marcats.

1.2. Objectius del Treball

L'objectiu d'aquest TFM es crear una plataforma web que faciliti la signatura electrònica qualificada de documents PDF que un usuari tingui al núvol sense necessitat de tenir els certificats en local ni requereixi cap tipus d'instal·lació de software específic per a la realització de la signatura.
Un altre objectiu és demostrar com diversos servidors de recursos d'una tipologia diferent poden interactuar entre ells per tal d'oferir un nou servei compost pels recursos que aquests ofereixen.

Un altre punt molt important és com es tracta la seguretat en diferents punts de la plataforma. En primer lloc, tan l'accés a la pròpia plataforma com les integracions amb els diferents servidors de recursos es realitza a través del protocol HTTPS. A més, a través del protocol OAuth2 es garanteix que només s'accedeix als recursos dels serveis autoritzats prèviament per l'usuari segons l'abast seleccionat.
Els documents allotjats als diferents serveis del núvol no són enviats mai a altres servidors, tot i que sí que es descarreguen i tracten a la pròpia plataforma de CloudDocs. Això permet mantenir la confidencialitat dels documents del propi usuari.

També es busca que l'accés i la utilització de la plataforma sigui el més senzill possible per l'usuari. No es requereix cap tipus de registre en la plataforma, ja que realitza un Single Sign-On a través dels serveis d'identificació i autorització de Google a través del protocol OpenID Connect. Tampoc és necessari cap tipus d'instal·lació extra a part del propi navegador web. Els certificats que s'utilitzen en el procés de signatura de documents estan emmagatzemats al servei de signatura qualificada TrustedX de Safelayer Secure Communications S.A., d'aquesta manera no és necessari disposar dels certificats instal·lats en local en els dispositius que es vulgui treballar.

A la fase inicial, la plataforma s'integra amb serveis d'emmagatzematge de fitxers Google Drive i Dropbox i, pel que fa als serveis de custodia de claus i signatura, únicament està integrat amb TrustedX. S'ha intentat realitzar un disseny que pretén facilitar la ampliació de nous proveïdors dels serveis utilitzats.

1.3. Enfocament i mètode seguit

L'estratègia utilitzada per a la realització de TFM ha estat seguir les pautes marcades en les fases d'un projecte de software:

Fase 1: Definició de l'abast del projecte i pla de treball

Entendre quina és la finalitat del TFM plantejat, definir-ne l'abast del projecte i fins on es vol arribar. Definir la planificació del projecte per tal de poder aconseguir les fites dins del període marcat.

Fase 2: Anàlisis i especificació

Elaboració de l'anàlisi de requisits detallant els diferents casos d'ús i diagrames de seqüència que formen part de les funcionalitats del projecte.

Fase 3: Preparació de l'entorn

Valorar i decidir quines tecnologies s'utilitzaran per a la realització del projecte, recopilar documentació de totes les APIs a utilitzar, provisió d'un servidor d'aplicacions web, creació d'un repositori de control de versions.

Fase 4: Implementació

Implementació de l'aplicació web en funció de les decisions preses en les fases anteriors.

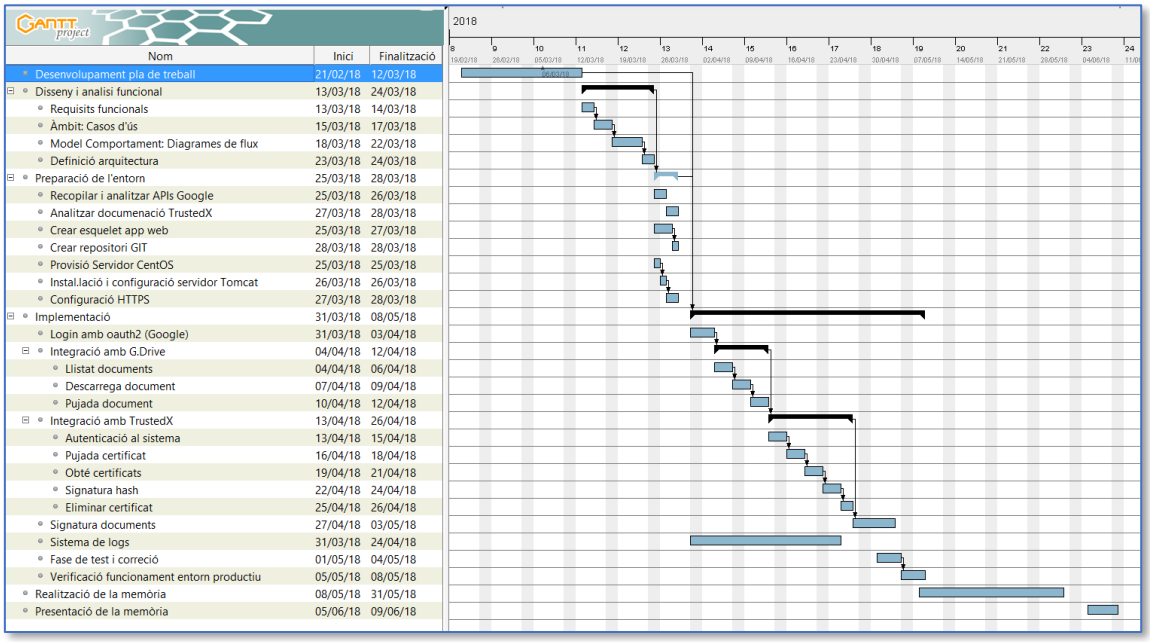
Fase 5: Realització de la memòria

Redacció del document de la memòria del TFM i preparació de la presentació virtual.

1.4. Planificació del Treball

La planificació de les diferents fases del projecte es pot veure detallada en el següent diagrama de gantt.

Aquest diagrama es va realitzar durant la fase de desenvolupament del pla de treball com a guia per a poder assolir les fites definides. Durant l'execució del projecte s'ha pogut escurçar el temps en algunes tasques, fet que ha permès la implementació d'algunes funcionalitats no contemplades inicialment.



Il·lustració 1 - Diagrama de gantt

1.5. Breu sumari de productes obtinguts

El TFM es divideix en les següents entregues parcials que formen part del resultat final del projecte:

- **PEC1:** Consisteix en detallar el pla de treball. En aquest es defineix el problema que es vol resoldre, els objectius que es volen assolir, la metodologia que s'utilitzarà i la descomposició i planificació de les tasques que es duran a terme.

- **PEC2:** Consisteix en la definició de l'anàlisi de requisits que conté el detall dels casos d'ús i els diagrames de flux d'aquests. Aquesta part és important per definir les funcionalitats que tindrà l'aplicació i com interactuaran amb els diferents actors del sistema.
  En aquest punt també es determina l'arquitectura i les tecnologies a utilitzar, es crea un esquelet d'allò que serà posteriorment l'aplicació i es comença amb la implementació de les funcionalitats.

- **PEC3:** Consisteix en completar la implementació del màxim de funcionalitats de l'aplicació per a tenir una versió molt avançada del demostrador. Al mateix temps es van documentant les decisions presses en la fase de disseny.

- **PEC4:** Consisteix en l'elaboració del document final de la memòria. Durant aquesta fase també es poleixen errors o mals funcionaments detectats a l'aplicació.

- **PEC5:** Consisteix en la realització d'una presentació virtual on s'exposa una síntesi del projecte i es realitza una demostració del funcionament de l'aplicació implementada.

1.6. Breu descripció dels altres capítols de la memòria

Els següents apartats de la memòria estan organitzats de la següent forma:

Arquitectura
Es descriu l'arquitectura de la plataforma, els components que la formen i la importància del protocol OAuth2.

Anàlisi de requisits
Es puntualitzen els diferents actors del sistema i els casos d'ús que s'implementaran. En aquesta part quedaran definides les característiques que tindrà el sistema.

Especificació
Es detalla la representació dels conceptes més significants del sistema i els diagrames de seqüència descrits en l'anàlisi requisits.

Disseny
Es determina el disseny dels diferents components que formen la capa de presentació i la capa de domini.

Implementació
S'enumera breument com s'ha realitzat la implementació del sistema i quines eines s'han utilitzat.

Demostració
Es mostra un exemple del flux que segueix un usuari des de l'accés a la aplicació fins la signatura d'un document, al mateix temps que s'especifica quins casos d'ús intervenen en cada moment.

Conclusions
Es precisen les conclusions del TFM juntament amb les reflexions sobre els objectius assolits i una anàlisi del seguiment del treball. A més a més , es proposen diferents millores que permetrien transformar aquest demostrador en un producte més complet.

Glossari
En el aquest apartat es defineixen els termes i acrònims més rellevants utilitzats dins la memòria del TFM.

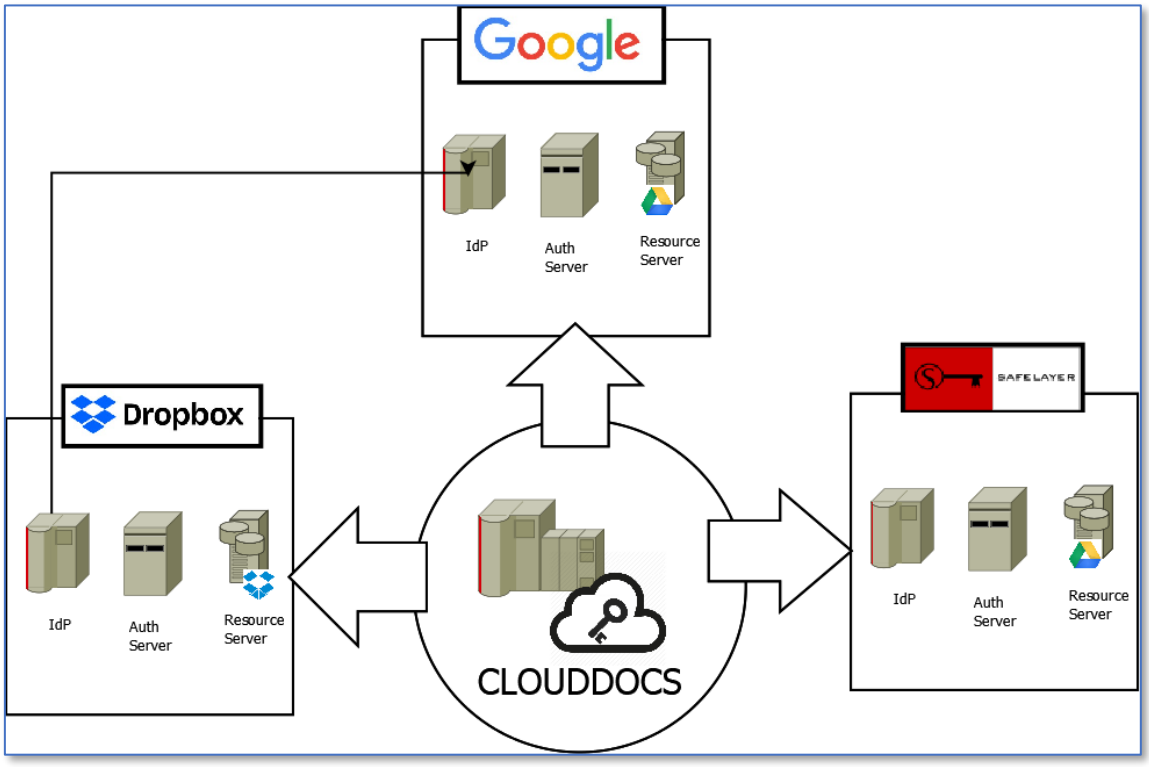
Bibliografia
Es llisten les diferents fonts externes d'informació utilitzades o referenciades en la memòria.

Annexos
Es delimiten els documents annexos que per extensió no es poden incloure dins la memòria.

2. Arquitectura

2.1. Visió general

En la següent il·lustració es mostra l'arquitectura de la plataforma CloudDocs en línies generals.



Il·lustració 2 - Diagrama arquitectura

En la part central del diagrama es troba un servidor web on s'executa l'aplicació CloudDocs. Al voltant d'aquest, s'ubiquen els diferents proveïdors de serveis on s'integra la plataforma.
Cadascun d'aquest proveïdors està format per almenys tres servidors que desenvolupen tasques ben diferenciades: autenticació (IdP) , autorització (Auth. Server) i prestació de recursos (Resource Server). El detall d'aquests servidors s'exposa en els apartats següents.
Les integracions amb els sistemes externs es realitzen utilitzant APIs REST a través del protocol HTTPS i basen la seva autorització amb el protocol OAuth2.

2.2. Identity Provider

Un Identity Provider (IdP), també anomenat Identity Service Provider or Identity Assertion Provider, és un servei en línia o un lloc web que autentica els usuaris a través d'internet. Uns dels protocols més utilitzats són OpenID i SAML.

2.2.1. OpenID

OpenID [7] [8] és un protocol d'identificació descentralitzat que permet als usuaris ser autenticats per llocs cooperatius, coneguts com Relying Parties o RP, utilitzant un servei de tercers. Aquest fet elimina la necessitat de tenir diferents comptes per accedir a diferents llocs web i amb una única identitats es pot accedir a diversitat de llocs.
Aquest protocol no especifica el mecanisme d'autenticació, per tant, la seguretat d'una connexió d'aquest tipus depèn de la confiança que tingui el client amb el proveïdor d'identitats utilitzat.

Aquest protocol ha tingut varies evolucions durant els últims anys:

- OpenID 1.x (2006) [9]
- OpenID 2.0 (2007) [10]
- OpenID Connect (2014) [11] [12]

2.2.2. Servidors

La plataforma CloudDocs interacciona amb els següents IdPs:

- Google Identity Provider

La plataforma CloudDocs utilitza el Google Identity Provider amb dues finalitats diferenciades:

- Obtenir la informació del perfil de l'usuari per accedir a CloudDocs.
- Verificar la identitat de l'usuari per obtenir posteriorment autorització per accedir als recursos de fitxers de Google Drive.

- Dropbox Identity Provider

La plataforma CloudDocs utilitza el Dropbox Identity Provider amb la finalitat següent:

- Verificar la identitat de l'usuari per obtenir posteriorment autorització per accedir als recursos de fitxers de Dropbox.

Resulta interessant puntualitzar que l'IdP de Dropbox es capaç de realitzar l'autenticació a través dels seus propis mecanismes o utilitzant l'IdP de Google per validar la identitat d'un usuari.

- TrustedX Identity Provider

La plataforma CloudDocs utilitza el TrustedX Identity Provider amb la finalitat següent:

- Verificar la identitat de l'usuari per obtenir posteriorment autorització per accedir als recursos d'identitats de TrustedX.

Aquest IdP també és capaç de realitzar l'autenticació a través de l'Idp de Google. tecnològicament es podria utilitzar una sola identitat per a realitzar la identificació als tres servidors de recursos, però a nivell normatiu no és possible.
El reglament eIDAS requereix un nivell de garantia alt en l'autenticació (LoA - Level Of Assurance) i l'IdP de Google no és capaç d'assolir-lo. A més, el nivell alt requereix la identificació electrònica d'utilitzar com a mínim dos factors d'autenticació de diferents categories (possessió, coneixement o inherents). Està dissenyat de tal manera que es pot assumir que l'usuari controla o té els factors d'autenticació. Per últim, el procés d'autenticació ha d'incloure l'autenticació dinàmica. [13] [14]

2.3. Authorization Server

Un authorizaltion server gestiona els accessos de clients a un servidor de recursos. Els límits que defineixen a quins recursos es té accés o no estan definits en els abasts (scopes) als quals l'usuari propietari del recurs n'ha autoritzat l'accés.
En el nostre cas, s'utilitza un servidor d'autorització per a cada servidor de recursos amb que s'integra la plataforma. El detall dels diferents abasts utilitzats i els recursos que ofereix cadascun d'ells està descrit als subapartats de l'apartat 2.4.

2.3.1. Protocol OAuth2

El protocol OAuth2 permet que les aplicacions de tercers concedeixin accés limitat a alguns dels seus serveis a un servei web http, ja sigui en nom del propietari dels recursos o permeten que l'aplicació de tercers obtingui accés per compte propi. El funcionament d'aquest consisteix en delegar l'autenticació d'usuaris al servei que allotja el compte d'usuari i autoritza les aplicacions de tercers per accedir al seu compte d'usuari en certs àmbits.

En el protocol defineixen quatre rols:

- Propietari del recurs (usuari)

El propietari del recurs és l' *usuari* que autoritza una *aplicació* per accedir al seu compte. L'accés de l'aplicació al compte d'usuari es limita al "abast" de l'autorització atorgada (p. Ex., Accés de lectura o escriptura).

- Servidor de recursos

El servidor de recursos allotja els comptes d'usuari protegits i el servidor d'autorització verifica la identitat de l' *usuari* i, a continuació, emet els tokens d'accés a l' *aplicació* .

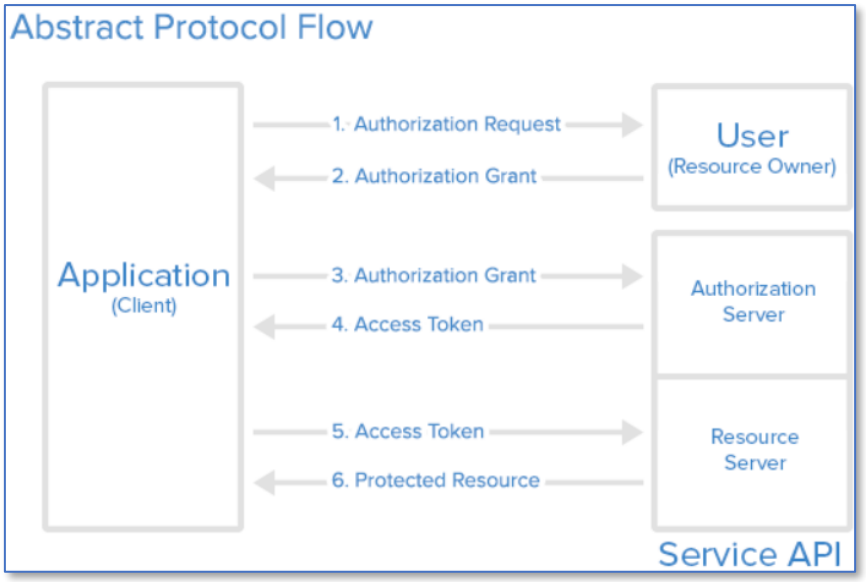
- Client

El client és l' *aplicació* que vol accedir al compte de l' *usuari* . Abans de poder fer-ho, ha d'estar autoritzat per l'usuari i l'autorització ha de ser validada per l'API.

- Servidor d'autorització

Servidor que envia token d'accés al client. Aquest testimoni s'utilitzarà perquè el client sol·liciti el servidor de recursos. Aquest servidor pot ser el mateix que el servidor d'autorització (el mateix servidor físic i la mateixa aplicació), i sovint és el cas.

En el següent esquema es descriu el flux de funcionament on interactuen els diferents rols descrits anteriorment.



Il·lustració 3 - Flux protocol OAuth2

Tot seguit teniu una explicació més detallada dels passos del diagrama:

1. La *Authorization request* sol·licita autorització per accedir als recursos del servei de l' *usuari*
2. Si l' usuari autoritza la sol·licitud, la *Authorization response* retorna un codi d'autorització
3. La *Authorization request* demana un token d'accés del *servidor d'autorització* (API) presentant l'autenticació de la seva pròpia identitat i l'ajut d'autorització
4. Si la identitat de l'aplicació està autenticada i la concessió d'autorització és vàlida, el *servidor d'autorització* (API) emet un token d'accés a l'aplicació. L'autorització s'ha completat.
5. L' *aplicació* sol·licita el recurs del *servidor de recursos* (API) i presenta el token d'accés per a l'autenticació
6. Si el token d'accés és vàlid, el *servidor de recursos* (API) serveix el recurs a l' *aplicació*

ES pot trobar informació més detallada a les següent referències. [15] [16]

En el cas de la plataforma CloudDocs, els rols quedarien de la següent forma.

- Propietari del recurs: l'usuari que accedeix a l'aplicació
- Servidor de recursos: Google Drive, Dropbox i TrustedX.
- Client: la pròpia aplicació CloudDocs
- Servidor d'autorització: els propis servidors de recursos també ofereixen les APIs per a realitzar l'autorització.

2.4. Resource Providers

Un resource provider és un proveïdor de serveis que ofereix certs recursos. El tipus dels recursos oferts defineix quina és la tipologia del servei, aquests poden ser de programari, d'infraestructura, de plataforma, etc.

Per accedir a aquests serveis es requereix una autenticació i autorització prèvia que s'obté a través dels passos indicats als apartats anteriors. Per tant, cadascun dels servidors de recursos llistats també disposen d'un Identity Provider i un authorization server per a realitzar aquestes tasques.

A continuació es detallen els serveis utilitzats per a cadascun dels proveïdors integrats amb la plataforma CloudDocs. És important remarcar que cada abast (scope) permet únicament l'accés als recursos que aquest té definits i que requereix l'autorització expressa de l'usuari per utilitzar-los.

Les següents taules mostren els abasts utilitzats en cada cas, el recurs que aquest ofereix i quines operacions permet. En alguns casos l'autorització permet l'accés als recursos durant un temps limitat i en altres cal autorització cada cop que s'utilitza, veurem en més detall les diferents casuístiques.

2.4.1. Google

Tal com s'ha comentat anteriorment, els recursos consumits a Google s'utilitzen per dues finalitats diferents.

En primer lloc, els abasts profile i email ens permeten recuperar la informació bàsica de l'usuari. Aquesta informació és la que s'utilitza en el procés d'autenticació a la plataforma CloudDocs i s'emmagatzema a la sessió d'usuari.

Àmbit	profile
Recurs	Informació bàsica del perfil
Accions	Consulta

Àmbit	email
Recurs	Adreça de correu electrònic
Accions	Consulta

Per altra banda, l'abast següent ens permet treballar amb els documents emmagatzemats a Google Drive.

Àmbit	https://www.googleapis.com/auth/drive
Recurs	Fitxers de l'usuari emmagatzemats a Google Drive
Accions	Consulta i gestió (creació, modificació i esborrat)

Es poden consultar tots els abasts que permet la API de Google a la següent URL https://developers.google.com/identity/protocols/googlescopes, d'aquesta forma es poden veure tots els recursos que ofereix Google.

2.4.2. Dropbox

En el cas de Dropbox, l'únic recurs que ofereix la seva API és la de poder treballar amb els fitxers emmagatzemats als seus servidors. La API oficial de Dropbox utilitzada no descriu exactament quin abast utilitza.

Àmbit	**únic, definit internament a la API*
Recurs	Fitxers de l'usuari emmagatzemats a Dropbox
Accions	Consulta i gestió (creació, modificació i esborrat)

2.4.3. TrustedX

El servei de TrustedX utilitzat és eSigP, aquest servei simplement custodia les claus amb els certificats (el que anomenem identitats) i realitza signatures del tipus PKCS#1 a partir d'un hash. S'ha triat aquest tipus de servei pels següents motius:

- Mantenim la confidencialitat dels documents, ja que la plataforma CloudDocs no envia el document sencer a una plataforma externa.
- Realitza la signatura en un menor temps, ja que només viatja el hash a través de la xarxa.

En aquest cas cal diferenciar dues finalitats en els abasts utilitzats. En primer lloc s'utilitzen els serveis per a registrar i gestionar les identitats (certificat + clau) de l'usuari.

Àmbit	urn:safelayer:eidas:sign:identity:registre
Recurs	Identitat
Accions	Registrar

Àmbit	urn:safelayer:eidas:sign:identity:manage
Recurs	Identitats
Accions	Gestionar (consulta i esborrat)

Per altre banda, aquest abast permet la utilització d'una identitat per a signar un document. Cada vegada que s'utilitzi aquest recursos es requereix l'autorització de l'usuari, per tant, el token obtingut és d'un sol ús.

Àmbit	urn:safelayer:eidas:sign:identity:use:server
Recurs	Identitat
Accions	Utilitzar una identitat per a signar

En aquest projecte s'ha optat per la utilització de certificats externs per al registre d'identitats. TrustedX també ofereix l'opció de generar identitats de signatura qualificades, ja que aquestes es generen directament al servidor.
L'elecció de l'ús de certificats externs ha estat motivada per a simplificar el demostrador i per tenir l'opció d'utilitzar certificats emesos per diverses entitats de certificació.

2.5. Seguretat

L'accés a l'aplicació es realitza sota el protocol HTTPS, en concret, utilitza un xifrat TLS 1.2.
Les integracions amb els servidors externs es realitzen a través de crides a serveis REST, ja sigui a través de les APIs oficials com en el cas de Google o Dropbox o utilitzant les classes que ofereix Spring per a realitzar les crides a TrustedX. Els accessos als endpoints REST també es realitzen sota el protocol HTTPS.
Aquest fet garanteix que la informació que viatja a través de la xarxa estigui xifrada i que no podrà ser interceptada i utilitzada per tercers no autoritzats.

3. Anàlisi de requisits

3.1. Actors i elements

Usuari
Són les persones que utilitzaran aquesta plataforma per a firmar els seus documents del cloud amb una signatura electrònica qualificada.

Proveïdor de serveis d'identificació
És el component que s'encarrega d'identificar els usuaris en un domini d'identitat.

Proveïdor de servei d'autorització
És el component que gestiona les autoritzacions que permeten als clients accedir a certs recursos.

Proveïdor de serveis de documents
És el component que proporciona un servei d'allotjament de fitxers al cloud.

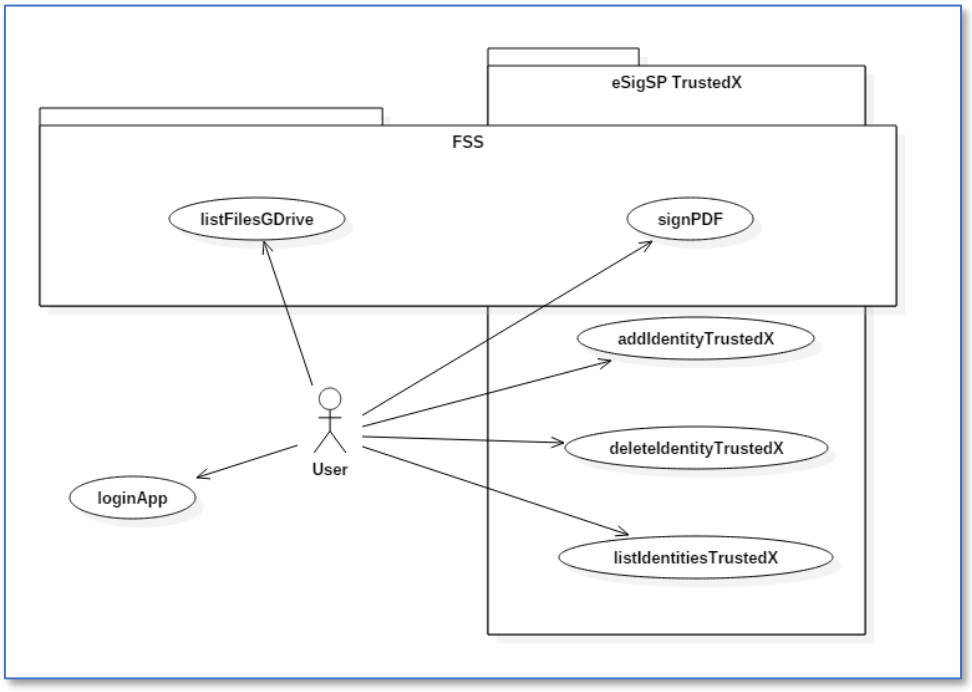
Proveïdor de serveis de signatura
És el component que ens proporciona un serveis de signatura electrònica qualificada de documents.

3.2. Àmbit

En aquest apartat s'identifiquen i s'especifiquen els casos d'ús del producte.

3.3. Diagrama casos d'ús

Un diagrama de cas d'ús és un tipus de diagrama de comportament. El seu propòsit és presentar un resum de forma gràfica de les funcionalitats que ofereix en sistema on es descriuen els actors, les finalitats i les dependències entre ells.



Il·lustració 4 - Diagrama Casos d'ús

3.4. Especificació casos d'ús

CU – 01	loginCloudDocs	
Dependències		
Precondicions	- L'usuari ha de tenir un compte amb Google - L'usuari ha accedit a la pantalla inicial de l'aplicació i ha clicat el botó d' iniciar sessió	
Descripció	L'usuari accedeix a l'aplicació CloudDocs, s'autentica al servidor IdP de Google i autoritza a l'aplicació a l'AS de Google en els scopes: perfil (profile), correu electrònic (mail) i G. Drive (https://www.googleapis.com/auth/drive)	
Seqüència	Pas	Acció
	1	L'usuari accedeix a l'aplicació i clica a log in
	2	El sistema sol·licita un codi d'autorització al AS de Google
	3	El sistema redirigeix l'usuari a la URL dels servidors de Google per iniciar OAuth.
	4	L'usuari s'autentica i concedeix l'autorització al sistema
	5	L'AS de Google retorna un codi d'autorització
	6	El sistema intercanvia el codi d'autorització pel token d'accés amb l'AS de Google.
	7	El sistema emmagatzema la informació retornada a la sessió
Postcondició	S'ha obtingut el token necessari per a realitzar peticions als servidors de Google que han estat autoritzats	
Excepcions	Pas	Acció
	3a	Es produeix un error en la redirecció (URL no autoritzada, servidors de Google no accessibles, etc.)
	4a	Credencials no vàlides
	4b	L'usuari s'identifica correctament però no accepta les autoritzacions
Comentaris		

CU – 02	listFilesGDrive	
Dependències	loginApp	
Precondicions	- L'usuari ha d'haver iniciat sessió a la plataforma i haver donat les autoritzacions als scopes de Google detallats al cas d'ús anterior - El sistema té emmagatzemat un token vàlid per aquest usuari	
Descripció	Es llisten els directoris i fitxers d'un directori seleccionat al FSS de Google Drive	
Seqüència	Pas	Acció
	1	L'usuari accedeix a l'apartat de veure fitxers, pagina o selecciona un directori concret ja mostrat
	2	La plataforma realitza la crida al FSS de Google Drive per a recuperar el llistat de fitxers que compleixi els filtres indicats per l'usuari utilitzant el token que ja tenia anteriorment
	3	El FSS de Google Drive retorna el llistat dels fitxers sol·licitats
	4	El sistema mostra els resultats

Postcondició	Es llisten per pantalla tots els fitxers i directoris corresponents.	
Excepcions	Pas	Acció
	2	Es produeix un error en la crida al FSS de Google Drive i no es poden llistar els documents sol·licitats.
Comentaris		

CU – 03	listFilesDropbox	
Dependències	loginApp	
Precondicions	- L'usuari ha d'haver iniciat sessió a la plataforma i haver donat les autoritzacions als scopes de Google detallats al cas d'ús anterior - El sistema té emmagatzemat un token vàlid per aquest usuari	
Descripció	Es llisten els directoris i fitxers d'un directori seleccionat al FSS de Dropbox	
Seqüència	Pas	Acció
	1	L'usuari accedeix a l'apartat de veure fitxers, pagina o selecciona un directori concret ja mostrat
	2	El sistema comprova si es disposa en sessió d'un token vàlid per a Dropbox. En cas afirmatiu se salta al pas 9.
	3	El sistema redirigeix l'usuari a l'AS de Dropbox per iniciar OAuth.
	4	L'AS de Dropbox sol·licita les credencials a l'usuari
	5	L'usuari s'autentica i concedeix l'autorització al sistema
	6	L'AS de Dropbox retorna un codi d'autorització
	7	El sistema intercanvia el codi d'autorització pel token d'accés amb l'AS de Dropbox.
	8	El sistema emmagatzema el token de Dropbox a la sessió d'usuari.
	9	La plataforma realitza la crida al FSS de Dropbox per a recuperar el llistat de fitxers que compleixi els filtres indicats per l'usuari utilitzant el token de Dropbox
	10	El FSS de Dropbox retorna el llistat dels fitxers sol·licitats
	11	El sistema mostra els resultats
Postcondició	Es llisten per pantalla tots els fitxers i directoris corresponents.	
Excepcions	Pas	Acció
	3a	Es produeix un error en la comunicació amb el servei de TrustedX.
	4a	Les credencials de l'usuari no són vàlides
	4b	L'usuari no accepta les autoritzacions sol·licitades
	9	Es produeix un error en la crida al FSS de Dropbox i no es poden llistar els documents sol·licitats.
Comentaris		

CU – 04	listIdentitiesTrustedX
Dependències	loginApp
Precondicions	- L'usuari ha d'haver iniciat sessió a la plataforma correctament.

Descripció	Es llisten tots els certificats disponibles per a realitzar la signatura electrònica qualificada	
Seqüència	Pas	Acció
	1	L'usuari accedeix a la secció 'Identitats de Signatura'
	2	L'usuari clica al botó 'Obtenir Identitats'
	3	El sistema redirigeix l'usuari a l'AS de TrustedX per iniciar OAuth.
	4	L'AS de TrustedX sol·licita les credencials a l'usuari
	5	L'usuari s'autentica i concedeix l'autorització al sistema
	6	L'AS de TrustedX retorna un codi d'autorització
	7	El sistema intercanvia el codi d'autorització pel token d'accés amb l'AS de TrustedX.
	8	El sistema realitza una petició a l'eSigP de TrustedX per tal de recuperar tots els certificats de l'usuari indicat.
	9	L'eSigP de TrustedX retorna una llista dels certificats disponibles per l'usuari indicat.
	10	El sistema emmagatzema aquesta informació per a mostrar-la a l'usuari a la pantalla corresponent.
Postcondició		
Excepcions	Pas	Acció
	3a	Es produeix un error en la comunicació amb el servei de TrustedX.
	5a	Les credencials de l'usuari no són vàlides
	5b	L'usuari no accepta les autoritzacions sol·licitades
	9a	L'usuari no té cap certificat al servei TrustedX
Comentaris		

CU – 05	addIdentityTrustedX	
Dependències	loginApp	
Precondicions	- L'usuari ha d'haver iniciat sessió a la plataforma i haver donat les autoritzacions corresponents. - El sistema té emmagatzemat un token vàlid per aquest usuari.	
Descripció	Es puja un certificat a la plataforma de servei de signatura avançada qualificada TrustedX.	
Seqüència	Pas	Acció
	1	El sistema sol·licita un certificat a l'usuari
	2	L'usuari selecciona un fitxer de certificat.
	3	El sistema realitza una petició a l'eSigP de TrustedX per tal d'emmagatzemar el certificat seleccionat per l'usuari indicat utilitzant el token que ja té.
	4	L'eSigP de TrustedX retorna si el resultat de la petició.
Postcondició	S'ha afegit el certificat seleccionat a la plataforma TrustedX de manera que ja pot ser utilitzat per a signar documents.	
Excepcions	Pas	Acció
	2a	El fitxer seleccionat per l'usuari no és vàlid.
	3a	Es produeix un error en la comunicació amb e l'eSigP de TrustedX.
	3b	El token utilitzant no és vàlid

	4a	Es produeix un error a l'emmagatzemar el certificat d'usuari a l'eSigP de TrustedX.
Comentaris		

CU – 06	deleteIdentityTrustedX	
Dependències	loginApp	
Precondicions	- L'usuari ha d'haver iniciat sessió a la plataforma i haver donat les autoritzacions corresponents. - El sistema té emmagatzemat un token vàlid per aquest usuari. - L'usuari ha de tenir algun certificat a l'eSigP de TrustedX	
Descripció	L'usuari esborra un certificat de l'eSigP de TrustedX que ja no vol utilitzar més.	
Seqüència	Pas	Acció
	1	El sistema recupera tots els certificats disponibles d'aquest usuari. (CU-04: listIdentitiesTrustedX)
	2	El sistema mostra els certificats a l'usuari.
	3	L'usuari selecciona quin certificat vol eliminar
	4	El sistema realitza una petició a l'eSigP de TrustedX per tal d'eliminar el certificat seleccionat per l'usuari utilitzant el token que ja té.
	5	L'eSigP de TrustedX retorna si el resultat de la petició.
Postcondició		
Excepcions	Pas	Acció
	4a	Es produeix un error en la comunicació amb e l'eSigP de TrustedX.
	4b	El token utilitzant no és vàlid
Comentaris		

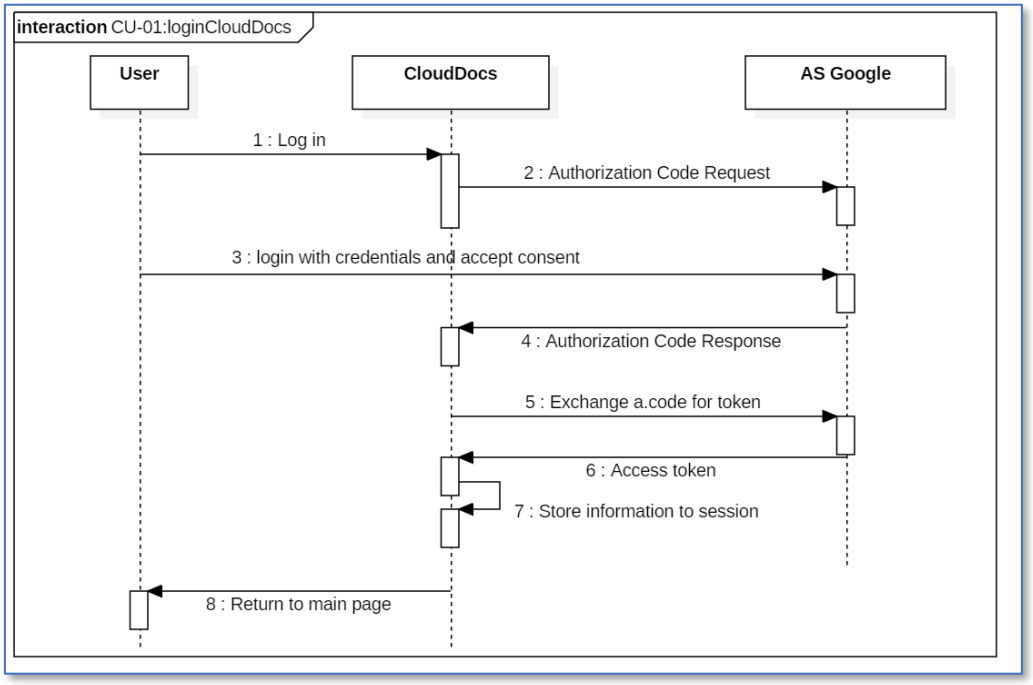
CU – 07	signDocument	
Dependències	loginCloudDocs listIdentitiesTrustedX	
Precondicions	- L'usuari s'ha d'haver iniciat sessió a la plataforma i haver donat les autoritzacions corresponents. - L'usuari ha seleccionat un document PDF per signar	
Descripció	Es realitza la signatura electrònica qualificada al document PDF indicat amb un dels certificats seleccionats per l'usuari.	
Seqüència	Pas	Acció
	1	L'usuari accedeix a l'opció 'Veure documents' i li apareixen els fitxers disponibles a G.Drive (*CU-02: listFilesGDrive*) o a Dropbox (*CU-03: listFilesDropbox*)
	2	L'usuari selecciona l'acció de signar un dels fitxers PDF mostrats en la llista anterior.
	3	El sistema recupera tots els certificats disponibles d'aquest usuari. (*CU-04: listIdentitiesTrustedX*)
	4	El sistema sol·licita a l'usuari que seleccioni amb quin certificat desitja fer la signatura electrònica qualificada.

	5	L'usuari selecciona el certificat
	6	El sistema redirigeix l'usuari a l'AS de TrustedX per iniciar OAuth.
	7	L'AS de TrustedX sol·licita l'autorització a l'usuari per l'scope signar.
	8	L'usuari concedeix l'autorització
	9	L'AS de TrustedX retorna un codi d'autorització
	10	El sistema intercanvia el codi d'autorització pel token d'accés.
	11	El sistema crida al FSS de G.Drive/Dropbox per a descarregar el document amb el token que ja té.
	12	El sistema calcula el hash del document.
	13	El sistema realitza la petició a l'eSigP de TrustedX per realitzar la signatura del hash calculat prèviament indicant quin certificat vol utilitzar
	14	L'eSigSP de TrustedX calcula i retorna el PKCS#1 resultant
	15	El sistema genera el PDF signat a partir del PDF original i el PKCS#1 retornat.
	16	El sistema crida al FSS de G.Drive/Dropbox per a emmagatzemar el document utilitzant el token que ja té
Postcondició	Et fitxer indicat per l'usuari ha estat signat i pujat a Google Drive	
Excepcions	Pas	Acció
	3a	Es produeix un error en la comunicació amb l'eSigP de TrustedX
	3b	L'usuari no té cap compte creada a l'eSigP de TrustedX
	3c	L'usuari no té cap certificat emmagatzemat a amb l'eSigP de TrustedX.
	8a	L'usuari no realitza l'autorització
	11a	Es produeix un error al descarregar el document del FSS de Google Drive.
	14a	Es produeixi un error al recuperar el PKCS#1 resultant, ja siguin problemes de xarxa o error del propi servei.
	14b	La identitat seleccionada ha caducat.
	15a	Es produeix un error l'analitzar i refer el PDF.
	15b	La signatura del PDF generat no és vàlida
	16a	Es produeix un error a l'emmagatzemar el document a Google Drive.
Comentaris		

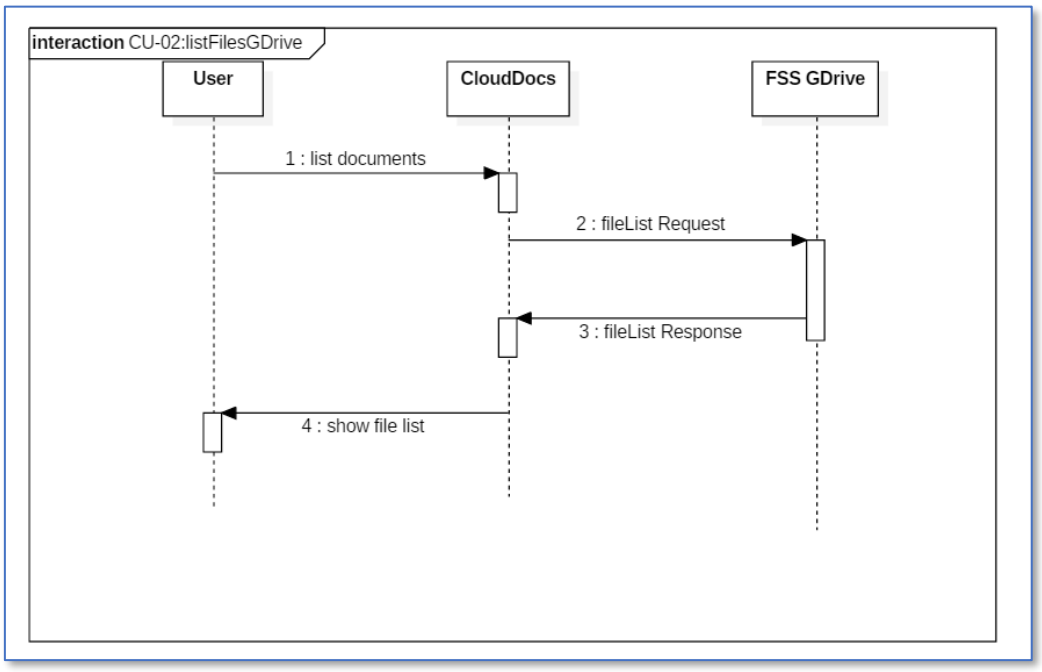
4. Especificació

4.1. Diagrames de seqüència

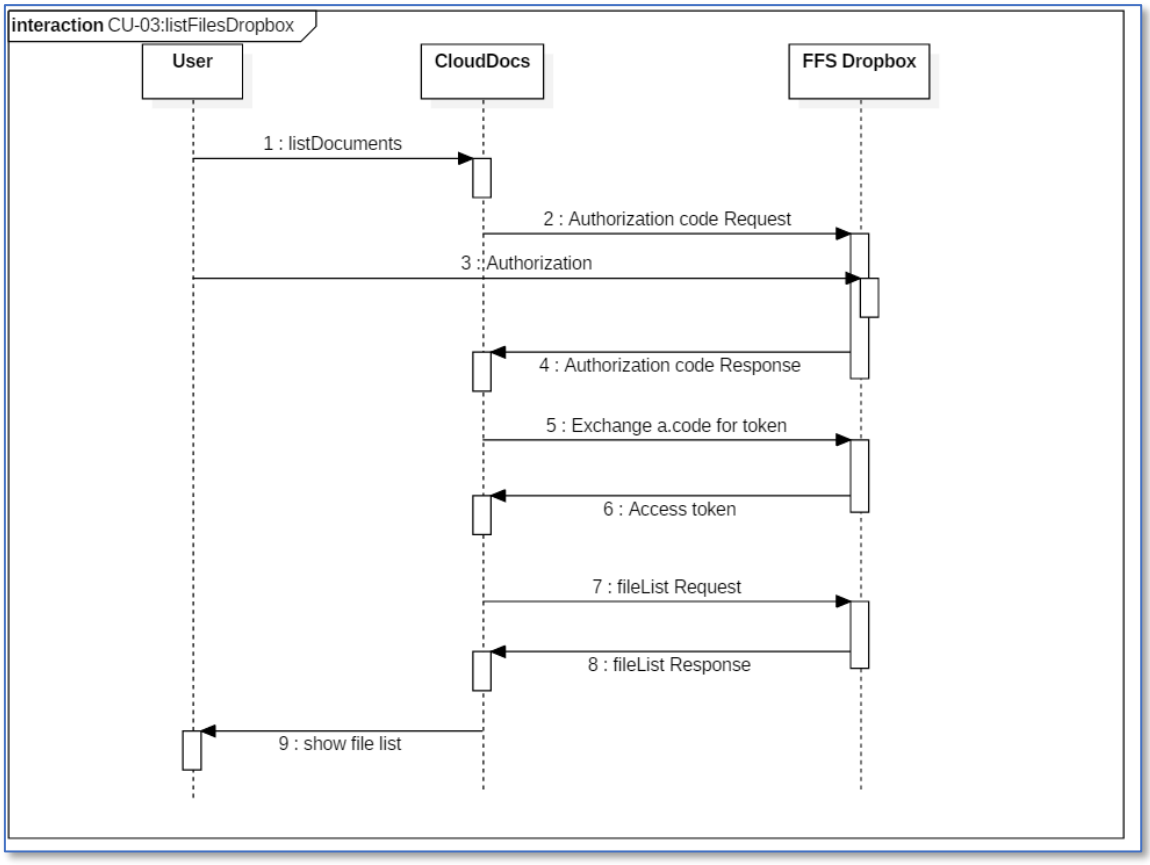
En aquesta secció es mostren els diagrames de seqüència descrits anteriorment a la secció 3.2



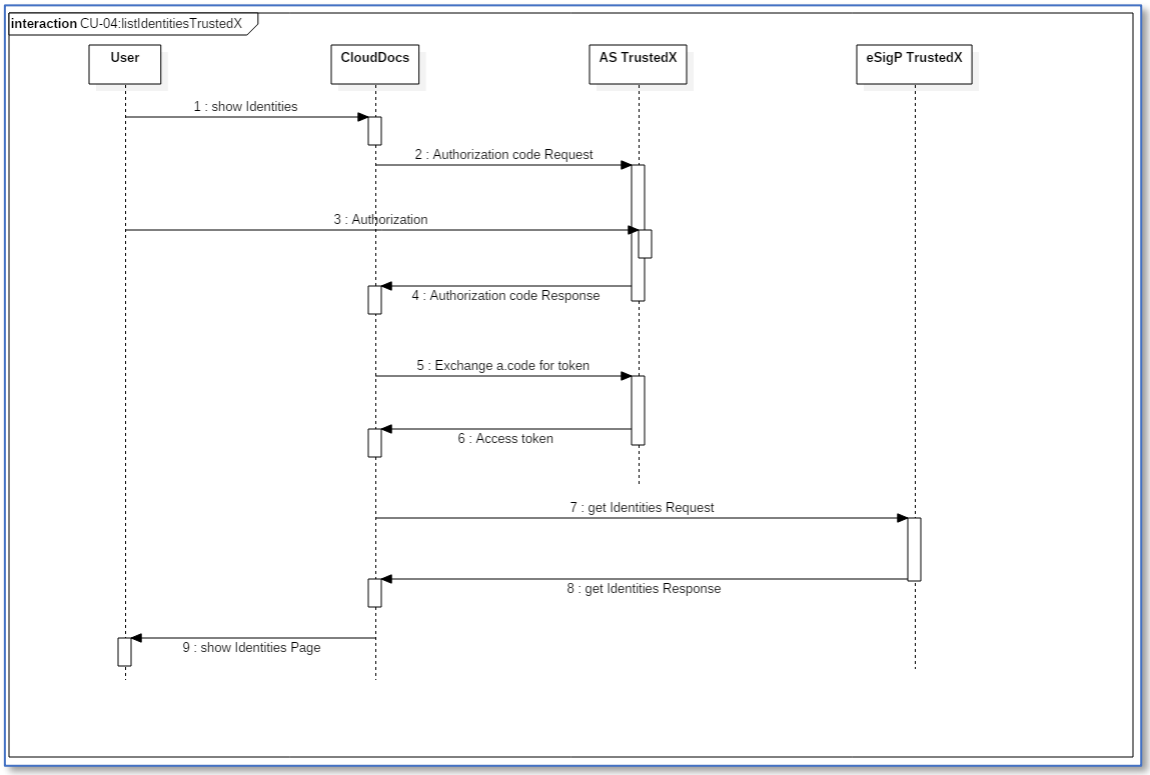
Il·lustració 5 - Diagrama de seqüència CU-01: loginCloudDocs



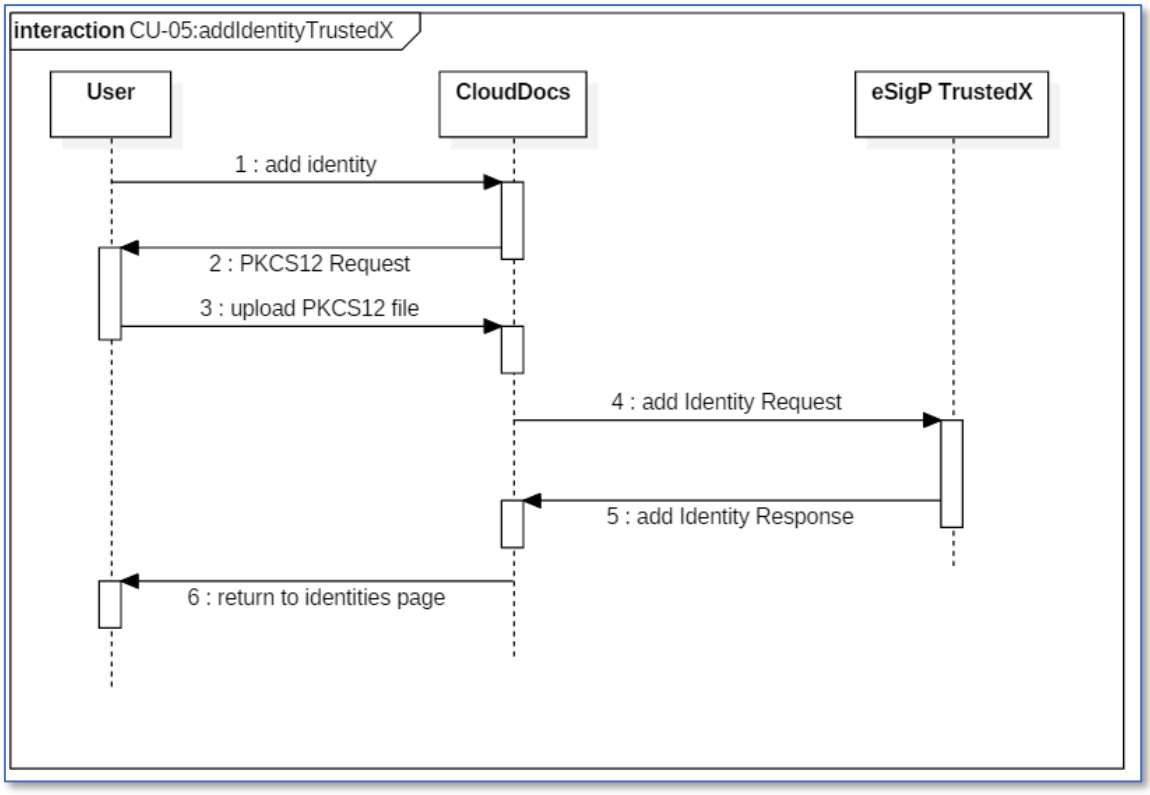
Il·lustració 6- Diagrama de seqüència CU-02: listFilesGDrive



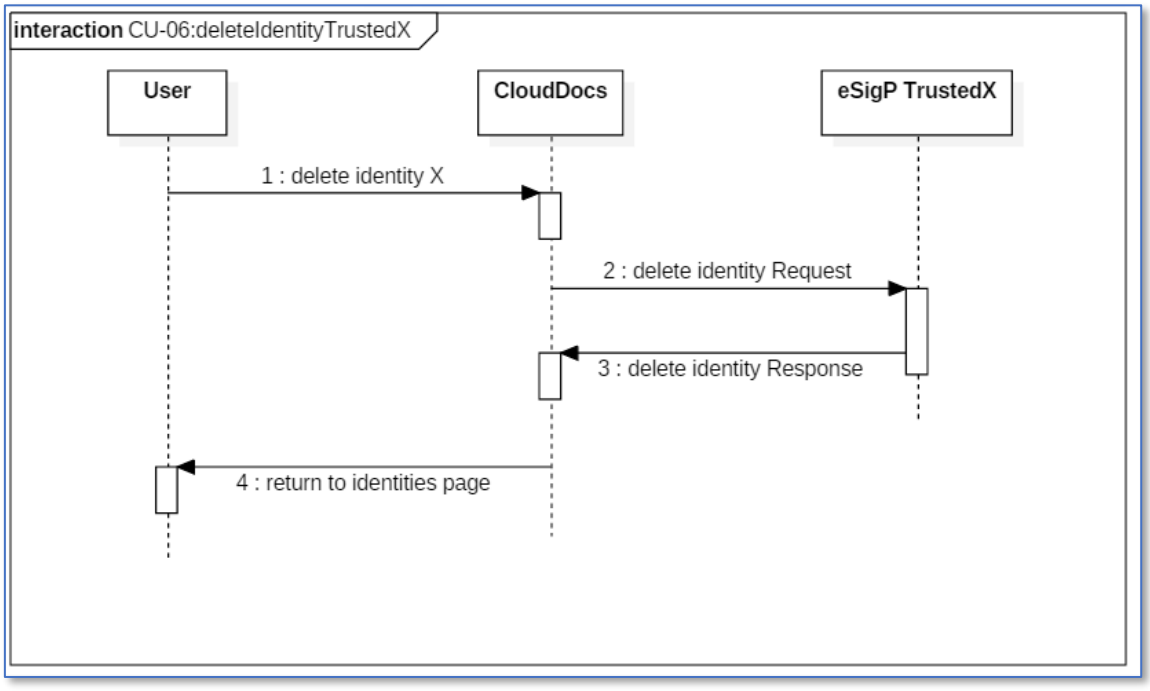
Il·lustració 7 - Diagrama de seqüència CU-03: listFilesDropbox



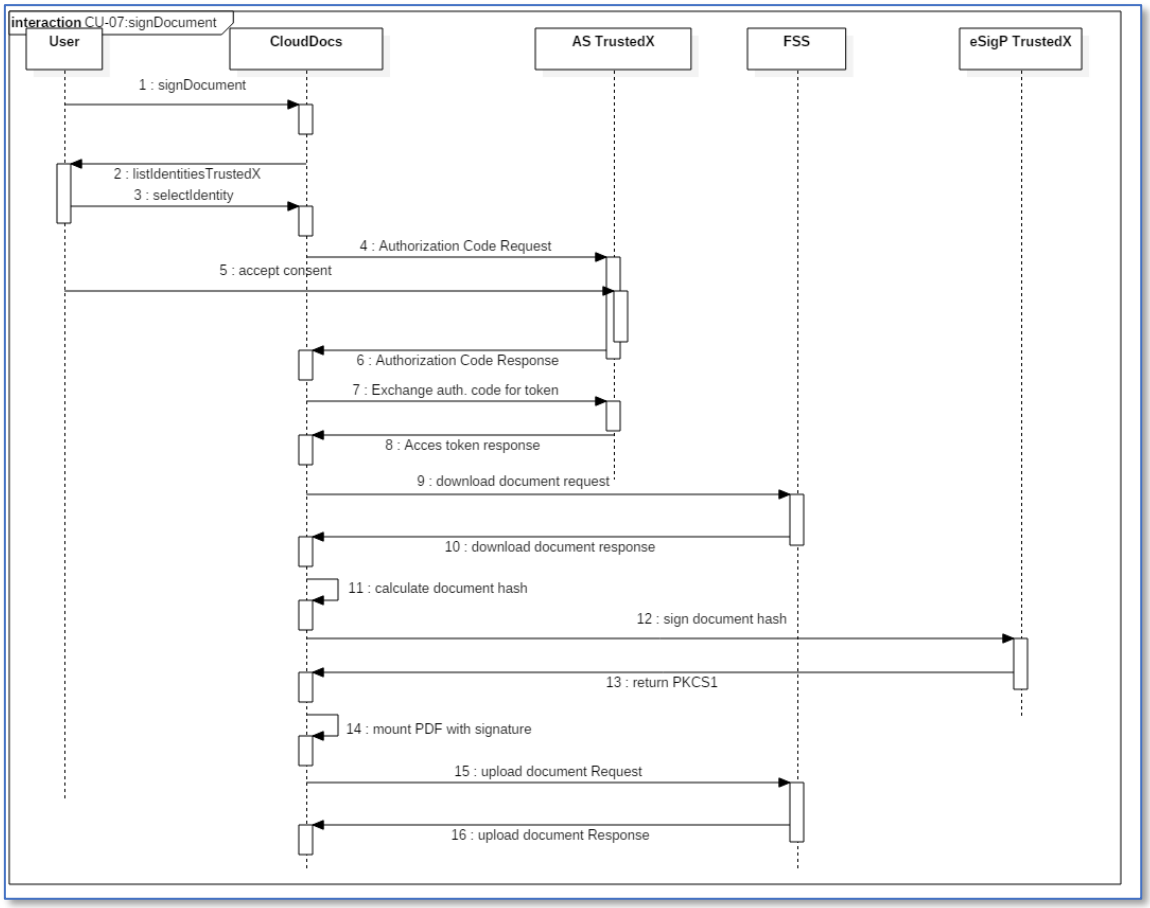
Il·lustració 8 - Diagrama de seqüència CU-04: listIdentitiesTrustedX



Il·lustració 9 - Diagrama de seqüència CU-05: addIdentityTrustedX



Il·lustració 10 – Diagrama de seqüència CU-06: deleteIdentityTrustedX



Il·lustració 11 – Diagrama de seqüència CU-07: signDocument

5. Disseny

5.1. Introducció

El disseny orientat a objectes és un refinament del model obtingut en el procés d'especificació. El que es vol és modelar l'arquitectura interna del sistema i identificar els seus components.

Una vegada que l'anàlisi dels requisits i l'especificació del programari es realitzen i són clars, s'han de triar les diferents opcions que ofereix l'Enginyeria del Software per obtenir una aplicació el més satisfactòria possible. Una decisió mai és definitiva, per tant, cal assolir l'equilibri entre els avantatges i els desavantatges que intervenen en les decisions.

Capa de presentació: ordena les execucions d'accions, recopila esdeveniments i gestiona la interfície. És el responsable de la interacció entre l'usuari i el sistema.

Capa de domini: executa les accions sol·licitades, obté els resultats i comunica les respostes a la capa de presentació i és responsable de l'aplicació de les funcionalitats del sistema.

5.2. Capa de presentació

En primer lloc s'han definit una sèrie de components compartits que s'utilitzen en les diferents vistes de l'aplicació per tal d'aprofitar el codi, facilitar-ne el manteniment, simplificar les vistes de l'aplicació, etc.

- **Header**

Es defineixen els meta atributs principals de la pàgina i s'importen els diferents fitxers d'estils (.css) necessaris.

- **Top**

Es defineix la barra principal de navegació on es mostra el botó de login o la informació de l'usuari en cas d'estar autenticat.

- **Menu**

Es defineix la barra secundària de navegació on es mostra el menú d'accés als diferents apartats de l'aplicació.

- **Ewi_messages**

Es mostren els diferents missatges d'error, advertència o informació en el cas que n'hi hagi (*ErrorWarnInfo messages*).

- **eSigP_list_select**

Es llisten tots els eSigP disponibles amb les identitats registrades per tal de poder seleccionar-ne una amb que signar els documents. Aquest component només s'importa a les vistes dels proveïdors de servei d'emmagatzemament de fitxers.

- **Footer**

Es defineix la barra de peu de la web i s'importen els fitxers Javascript comuns per a totes les pàgines.

Per altre banda determinat les vistes necessàries per a cada funcionalitat o proveïdor concret.

- **Index**

Pàgina d'accés a l'aplicació on es mostren les funcionalitats bàsiques que aquesta ofereix.

- **Dashboard**

Pàgina principal d'un usuari autenticat al sistema on es llisten els apartats més destacats.

- **listTrustedXIdentities**

Pàgina on es fa una relació de les identitats registrades per l'usuari autenticat amb TrustedX de Safelayer. En aquesta vista també es permet registrar noves identitats o esborrar-ne d'existents.

- **listDocumentsDropbox**

Pàgina on es llisten els directoris i fitxers disponibles per a l'usuari autenticat a Dropbox. En aquesta es poden llistar, descarregar i signar documents.

- **listDocumentsGDrive**

Pàgina on es llisten els directoris i fitxers disponibles per a l'usuari autenticat a Google Drive. En aquesta es poden llistar, descarregar i signar documents.

- **errors**

Diferents vistes per a tractar els errors que poden produir-se al sistema.

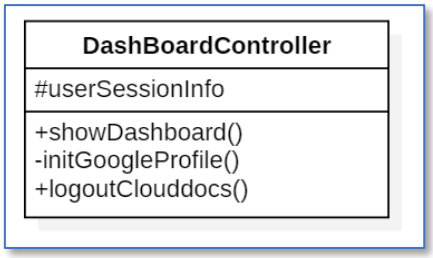
5.3. Capa de domini

5.3.1. Controladors

Aquests controladors es poden dividir en tres categories: pàgina inicial, servei d'emmagatzematge de fitxers i proveïdors de signatura de fitxers.

- **Pàgina inicial**

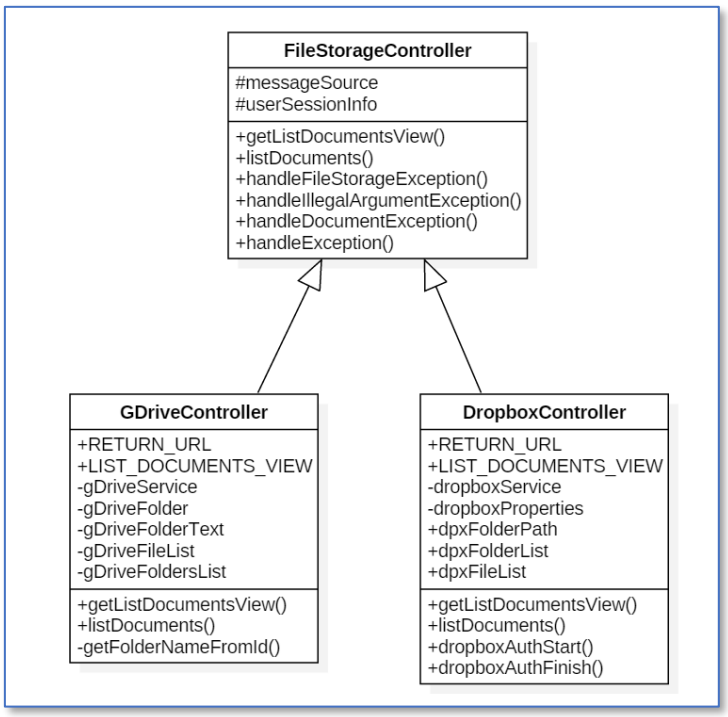
Aquest controlador simplement és el punt d'entrada a l'aplicació un cop s'ha autenticat l'usuari on inicialitza les dades de sessió, també permet realitzar el tancament de sessió.



Il·lustració 12 – Disseny classe DashBoadController

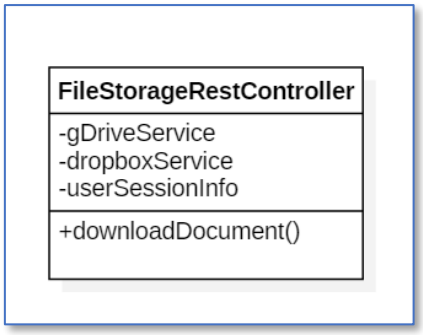
- **Servei d'emmagatzematge de fitxers (FSS)**

La classe FileStorageController defineix les funcionalitats bàsiques d'un controlador d'un FSS. Qualsevol nou FSS que s'afegeixi al sistema caldrà que implementi aquesta classe.
Les classes GDriveController i DropboxController implementen la classe FileStorageController amb les seves particularitats per adaptar-se al servei amb que es connecten.



Il·lustració 13 - Disseny classes FileStorageControllers

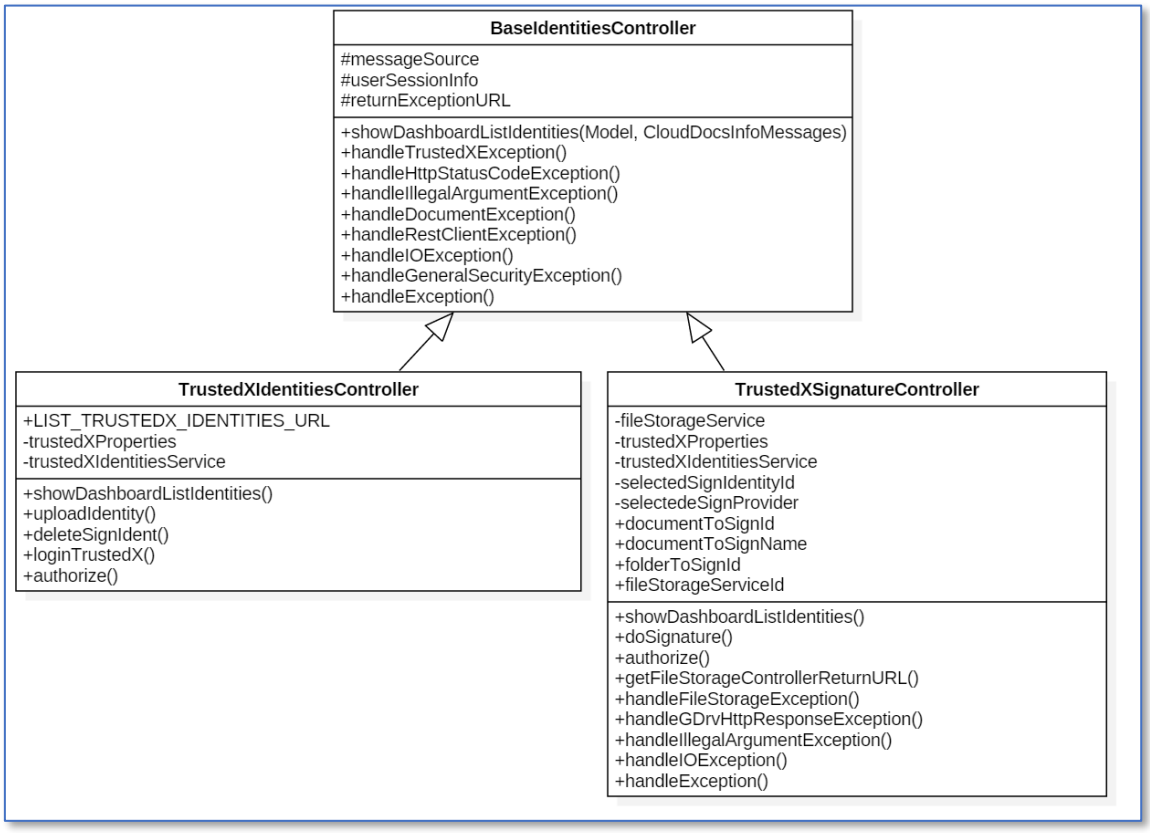
La classe FileStorageRestController ofereix uns serveis REST com a únic punt d'entrada per a la descàrrega de documents de qualsevol FSS.



Il·lustració 14 - Disseny classes FileStorageRestController

- **Proveïdors de signatura de fitxers (eSigP)**

La classe BaseIdentitiesController defineix les funcionalitats bàsiques d'un controlador d'un eSigP. Qualsevol nou eSigP que s'afegeixi al sistema caldrà que implementi aquesta classe.
Per a cada eSigP Caldrà definir dos controladors: un per a gestionar-ne les identitats (llistar, afegir i esborrar) com és la classe TrustedXIdentititesController i una altre classe per a la realització de signatures com és la classe TrustedXSignatureController



Il·lustració 15 - Disseny classes IdentitiesController

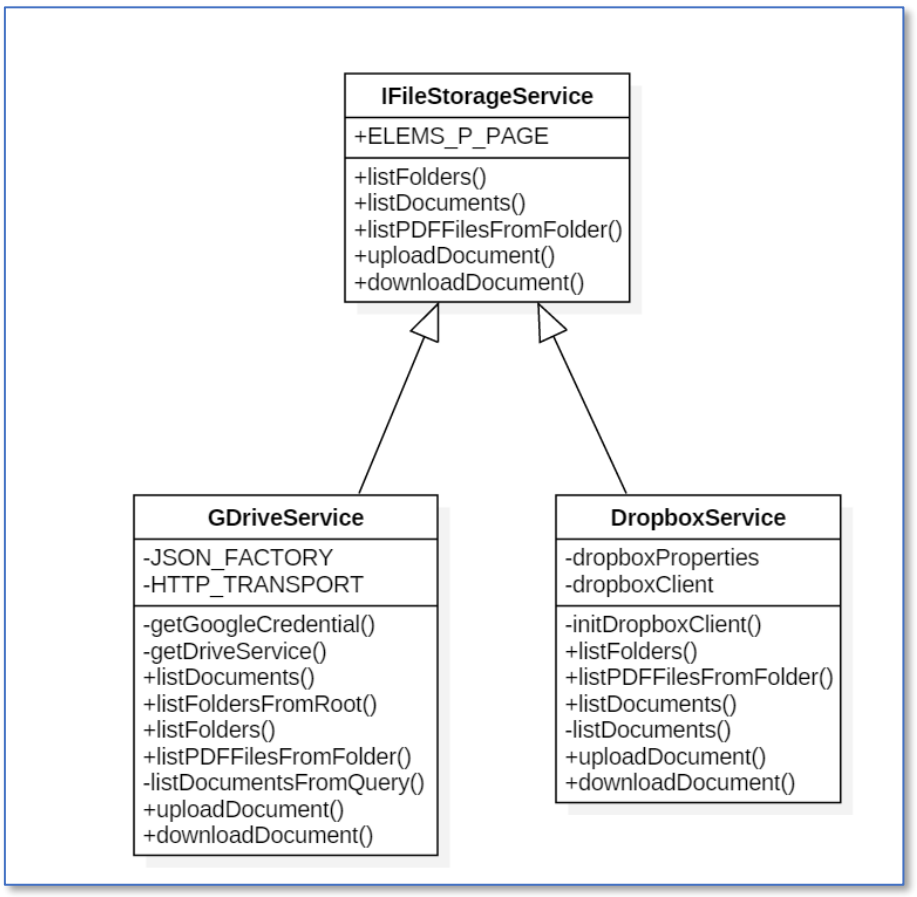
La classe IdentitiesRestController ofereix uns serveis REST com a únic punt d'entrada a la recuperació de les identitats de signatura per als controladors dels FSS. També disposa d'un servei per a emmagatzemar a la sessió d'usuari l' última identitat seleccionada.

Il·lustració 16 - Disseny classe IdentitiesRestController

5.3.2. Serveis

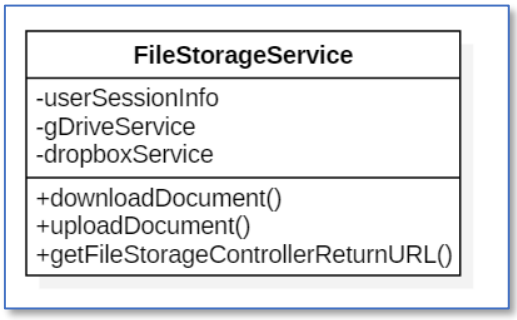
- **Servei d'emmagatzematge de fitxers (FSS)**

En primer lloc es defineix la interfície IFIleStorageService amb els mètodes mínims que qualsevol servei de FSS haurà d'implementar.
Posteriorment es defineixen els serveis específics per a cada un dels serveis (Google Drive i Dropbox) que implementen els mètodes de la interfície i altres mètodes propis.



Il·lustració 17 - Disseny classes FileStorageServices

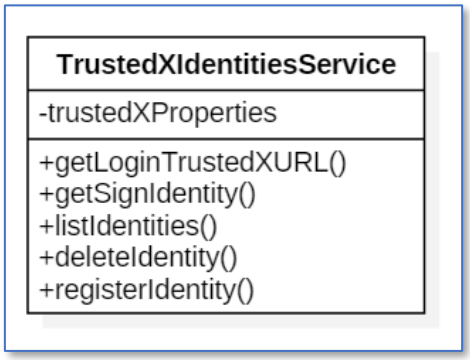
La classe FileStorageService actua com a únic punt d'entrada per a la descàrrega i pujada de documents independentment del FSS.



Il·lustració 18 - Disseny classe FileStorageService

- **Proveïdors de signatura de fitxers (eSigP)**

En aquest cas només hi ha un eSigP definit a la classe TrustedXIdentititesService que disposa dels mètodes necessaris per a la gestió d'identitats.



Il·lustració 19 - Disseny classe TrustedXIdentitiesService

6. Implementació

6.1. Signatura de documents

La implementació de la signatura de documents mereix un apartat específic on detallar-ne la implementació i el per què d'aquestes decisions, al cap i a la fi, es tracta del servei afegit principal que ofereix la plataforma CloudDocs.

Per a realitzar la signatura dels documents s'ha utilitzat el servei de TrustedX. Resulta interessant conèixer quins serveis concrets ofereix aquesta empresa, els seus detalls i explicar posteriorment perquè s'ha escollit un d'ells.

- **eSigP**
- Custodia les identitats de firma (certificats digitals i les seves claus).
- Realitza signatures a partir d'un resum criptogràfic d'un document en format PKCS#1.

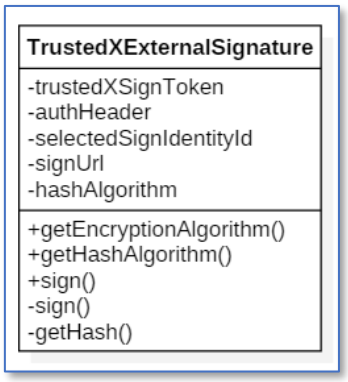
- **eSignSP**
- Realitza signatures a partir d'un document complet i les identitats custodiades per l'eSigP. És capaç de calcular el resum criptogràfic, realitzar la signatura i generar el document PDF signat.

L'opció escollida per a la plataforma CloudDocs ha estat eSigP pels següents motius:

- Mantenim la confidencialitat dels documents, ja que la plataforma CloudDocs no envia el document sencer a una plataforma externa.
- Realitza la signatura en un menor temps, ja que només viatja el hash del document a través de la xarxa.

Aquesta elecció implica que ha sigut necessari implementar un component capaç de generar el resum criptogràfic, enviar-lo a la plataforma TrustedX, obtenir-ne la signatura PKCS#1 i construir el fitxer PDF signat.

Per realitzar tot el procés de la signatura he utilitzat la API de Java iText, en concret la versió 5.5.13. Ha estat necessari implementar la classe ExternalSignature per tal de personalitzar el comportament del mètode sign que genera la signatura en si, però al mateix temps utilitzar la API de iText per al tractament dels documents PDFs.



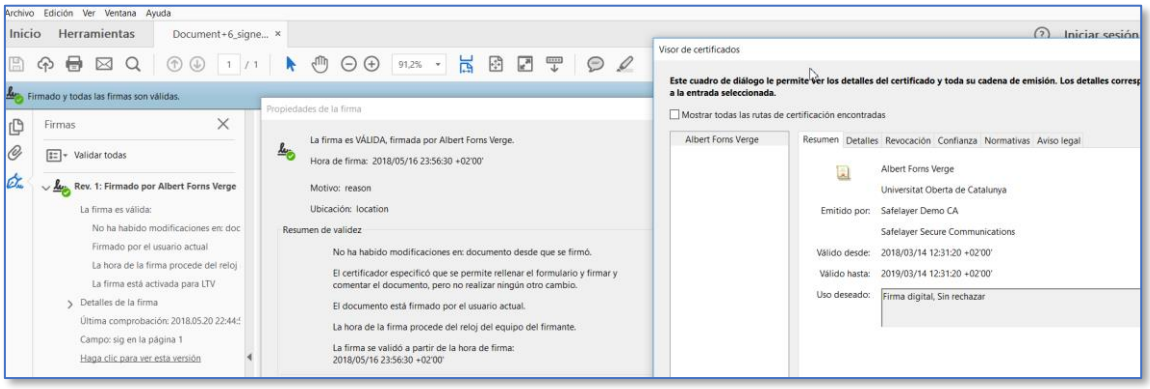
Il·lustració 20 - Disseny classe TrustedXExternalSignature

Els passos que segueix aquest mètode són:

- Generar el resum criptogràfic amb l'algoritme SHA-512
- Crida al servei REST de TrustedX
- L'usuari autoritza l'accés al recurs identitat per a realitzar la signatura.
- Recupera la signatura PKCS#1
- Genera el document PDF signat

Cal tenir en compte que per a poder generar el PDF signat amb el certificat corresponent a la identitat seleccionada, prèviament s'ha realitzat una crida a la API Rest de TrustedX per a obtenir el certificat en format X.509 per afegir-lo al document PDF resultant.

Les signatures resultants han estat validades amb el visor de PDFs Acrobat Reader, el qual és utilitzat per la gran majoria d'usuaris per a visualitzar documents d'aquest tipus.

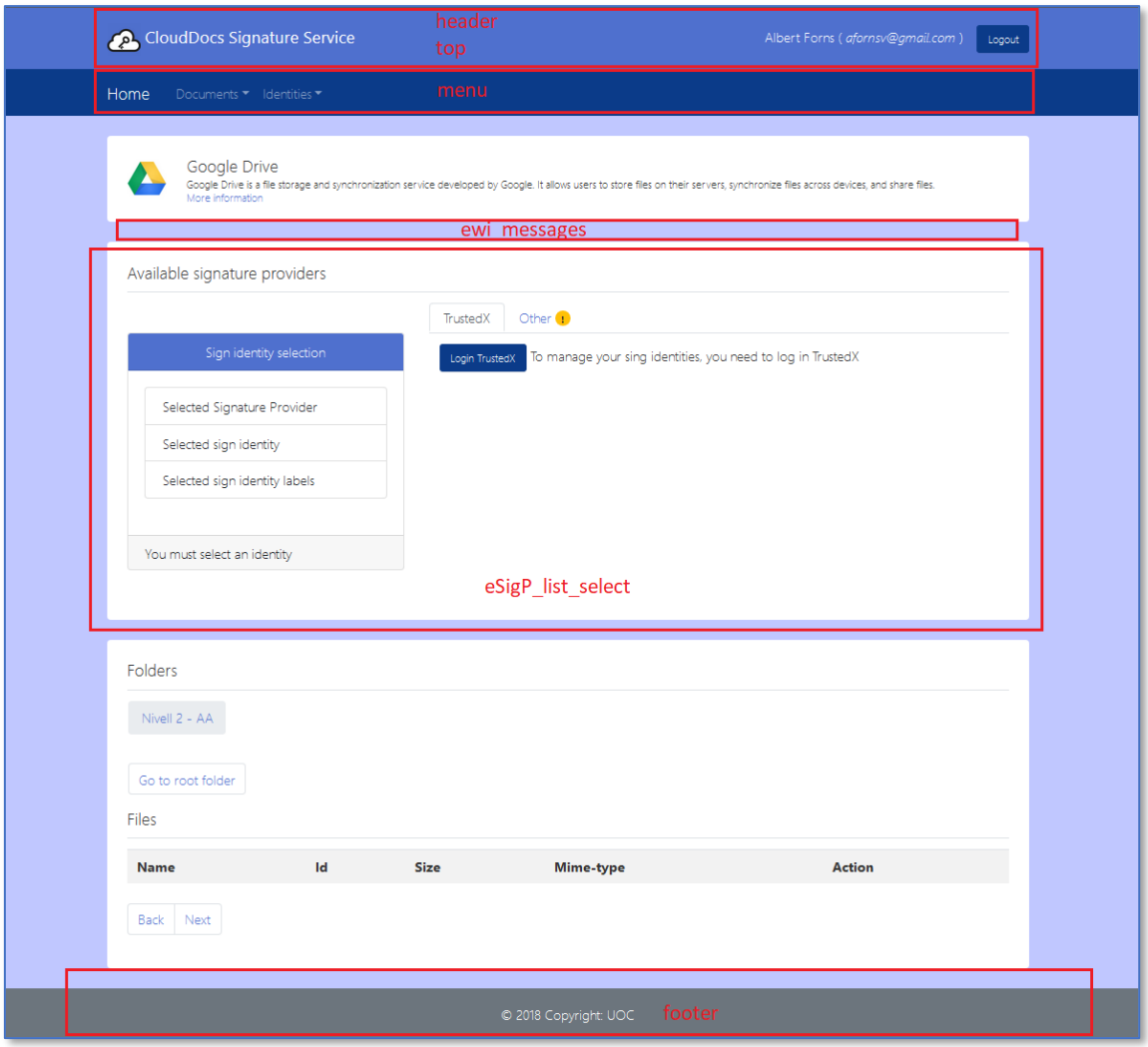


Il·lustració 21 - Verificació signatura en document PDF resultant

El document PDF signat compleix l'especificació de la signatura PDF ISO-32000-1 [17] que defineix els estàndards d'aquest format.

6.2. Capa de presentació

En la implementació de la capa de presentació s'ha utilitzat el motor de plantilles server-side Java per a entorns web anomenat Thymeleaf. L'objectiu ha estat poder crear unes plantilles d'una forma ben estructurada i ben formatada.
La següent imatge mostra una de les vistes del demostrador web on es detalla la ubicació d'alguns dels components compartits entre les vistes.



Il·lustració 22 - Esquema plantilles capa presentació

6.3. Capa de domini

En la implementació de la capa de domini s'ha utilitzat el framework Spring. Els elements principals utilitzats en aquesta capa són els següents:

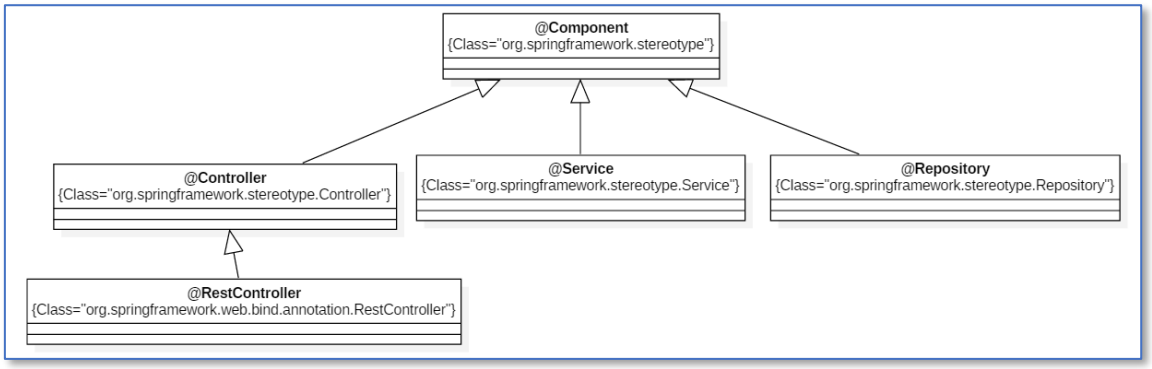
@Component: Estereotip genèric per qualsevol component o bean gestionat per Spring.

@Repository: Estereotip per a la capa de persistència. En aquest projecte no ha estat utilitzat però caldria tenir-ho en compte per a la implementació dels treballs futurs descrits en l'apartat 7.1.

@Service: Estereotip per a la capa de serveis

@Controller: Estereotip per a la capa de presentació (MVC)

@RestController: Estereotip per a la creació de serveis web RESTful.



Il·lustració 23 - Esquema classes utilitzades (Spring)

@EnableOAuth2Sso: Gestionar el Single Sign-On a través de OAuth2, en aquest cas amb el servei d'identitat de Google. La parametrització està definida al fitxer application.yml.

@Scope("session"): Indica que el component s'emmagatzema a la sessió d'usuari.

@PropertySource: Gestiona els paràmetres emmagatzemats en un fitxer.

6.4. Tecnologies i eines utilitzades

Per a la implementació d'aquest TFM he utilitzat les següents eines:

Spring boot	
Descripció	És un projecte d'Spring que ens ajuda la creació de noves aplicacions/projectes basats en Spring de forma àgil i evitar configuracions repetitives. Està centrat en el desenvolupament de l'aplicació facilitant la part de configuracions, llibreries, desplegament, etc.
Enllaços d'interès	https://projects.spring.io/spring-boot/

Thymeleaf	
Descripció	És un motor modern de plantilles de servidor Java per a entorns web i independents. L'objectiu principal de Thymeleaf és portar elegants plantilles naturals al vostre flux de treball de desenvolupament: un codi HTML que es pot mostrar correctament en els navegadors i que també funciona com a prototips estàtics, cosa que permet una major col·laboració en equips de desenvolupament.
Enllaços d'interès	https://www.thymeleaf.org/

iText	
Descripció	És un conjunt de llibreries per a crear i manipular fitxers PDF, en aquest cas ge utilitzat la versió 5.
Enllaços d'interès	https://itextpdf.com/

maven	
Descripció	És una eina de gestió i comprensió de projectes de programari. Basat en el concepte d'un model d'objectes de projecte (POM), Maven pot gestionar la construcció, l'elaboració d'informes i la documentació d'un projecte a partir d'una informació central.
Enllaços d'interès	https://maven.apache.org/

API Google	
Descripció	Són un conjunt de llibreries que faciliten la realització i gestió de crides REST a les APIs de Google i Google Drive.
Enllaços d'interès	https://developers.google.com/identity/protocols/OAuth2 https://developers.google.com/drive/v3/web/about-sdk

API Dropbox	
Descripció	Són un conjunt de llibreries que faciliten la realització i gestió de crides REST a les APIs de Dropbox.
Enllaços d'interès	https://www.dropbox.com/developers/documentation/java

Pingendo	
Descripció	És una aplicació per a la creació d'interfícies web basades en bootstrap.
Enllaços d'interès	https://pingendo.com/

JQuery	
Descripció	És una biblioteca Javascript que facilita la implementació en aquest llenguatge.
Enllaços d'interès	https://jquery.com

Bootstrap	
Descripció	És un toolkit open source per al desenvolupament amb HTML, CSS i JS.
Enllaços d'interès	https://getbootstrap.com/

Font Awesome	
Descripció	És un Toolkit que conté un conjunt d'icones per a utilitzar-los en la web.
Enllaços d'interès	https://fontawesome.com/

Star UML	
Descripció	Eina utilitzada per a la creació de diagrames UML. És compatible amb l'estàndard UML 2.x i suporta 11 tipus de diagrames UML: classe, objecte, cas d'ús, component, implementació, estructura composta, seqüència, comunicació, diagrama d'estat, activitat i diagrama de perfil.
Enllaços d'interès	http://staruml.io/

Spring Tool Suite	
Descripció	Spring Tool Suite és un entorn de desenvolupament basat en Eclipse personalitzat per desenvolupar aplicacions en Spring. Proporciona un entorn preparat per a implementar, depurar, executar i implementar les aplicacions Spring.
Enllaços d'interès	http://spring.io/tools/sts http://www.eclipse.org/downloads/

Gantt Project	
Descripció	Aplicació per a la programació i gestió de projectes.
Enllaços d'interès	http://www.ganttproject.biz/

GIT	
Descripció	Eina per al control de versions
Enllaços d'interès	https://bitbucket.org/ https://git-scm.com/

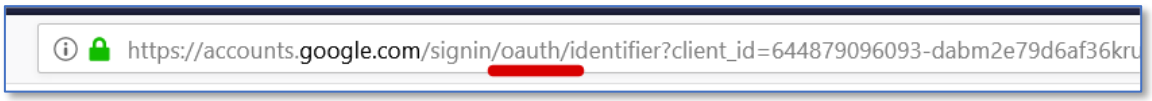
7. Demostració

En aquest apartat es mostra la interacció d'un usuari amb la plataforma CloudDocs al mateix temps que es detalla a quin cas d'ús correspon cada acció i quin és el comportament de cada component.

El primer pas consisteix en accedir a la plataforma i autenticar-se amb un usuari vàlid. A la vista inicial cal clicar al botó 'Sig in with Google', en aquest moment s'executen les accions definides al cas d´ús CU-01. La plataforma ens redirecciona a la URL d'autenticació del servidor IdP de Google.

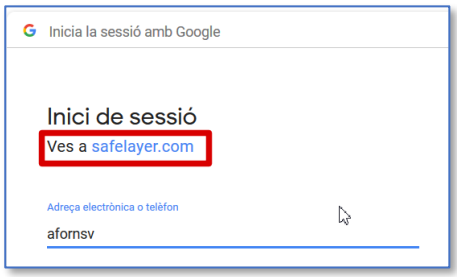
Il·lustració 24 - Vista login a la plataforma CloudDocs

La API de Google utilitza el protocol OpenID Connect [11] per a realitzar l'autenticació a través del serveis del seu servidor IdP.

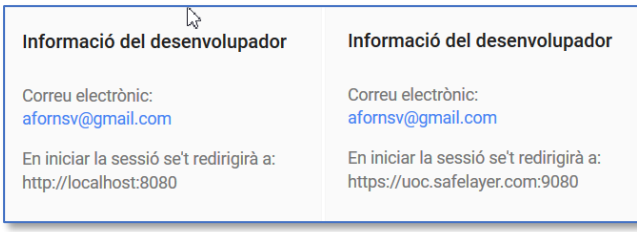


Il·lustració 25 - URL redirecció oauth IdP Google

Posteriorment a la vista on es sol·licita l'usuari i contrasenya es mostra la URL de l'aplicació que està sol·licitant l'autenticació. En aquest punt s'estan autoritzant a la plataforma els abasts profile i email.
Es pot observar l'àmbit diferent segons si l'execució és en l'entorn local de desenvolupament (http://localhost:8080/) o en el servidor de l'entorn de producció (https://uoc.safelayer.com:9080)

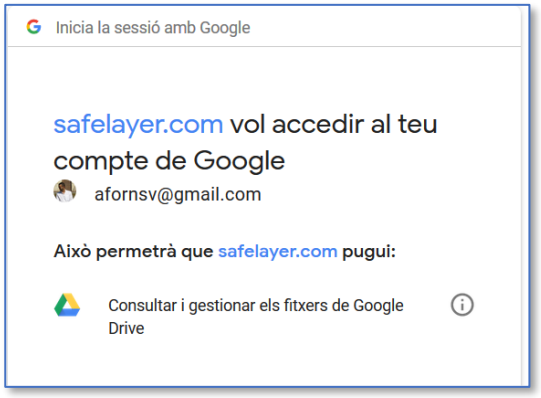


Il·lustració 26 - Vista autenticació a Google

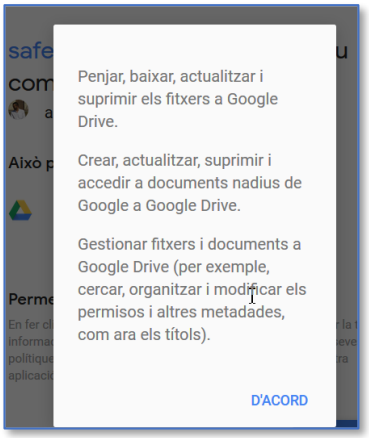


Il·lustració 27 - Informació aplicació autenticació Google

Una vegada autenticats es mostra una nova vista per tal d'autoritzar a la plataforma CloudDocs a accedir als recursos de Google Drive de l'usuari tal com s'observa a la següent il·lustració. L'abast que està autoritzant en aquest punt és https://www.googleapis.com/auth/drive, es pot consultar el detall de que estem autoritzant exactament clicant a la icona d'informació.

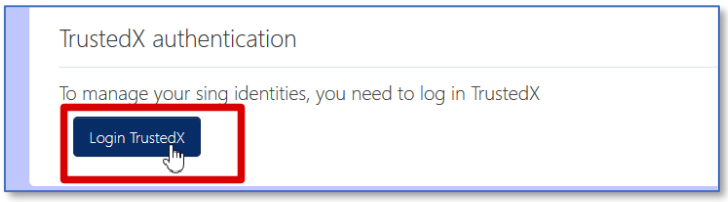


Il·lustració 28 - Vista autorització abast Google Drive



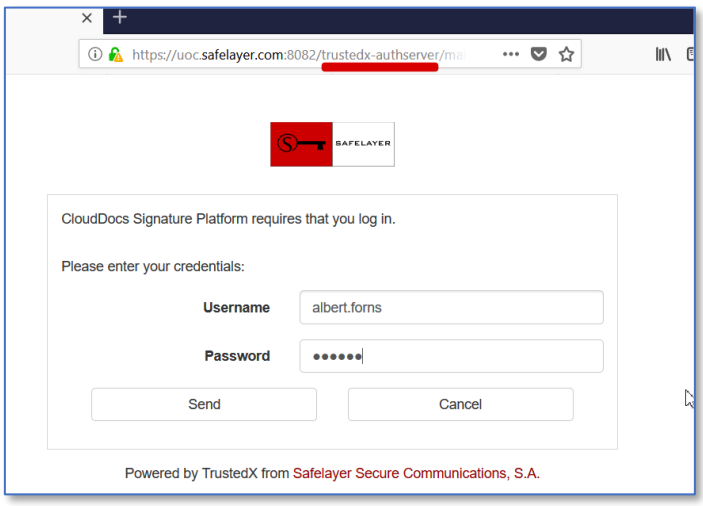
Il·lustració 29 - Recursos autoritzats abast Google Drive

Un cop autenticats a l'aplicació i amb l'autorització per accedir als fitxers PDF ubicats a Google Drive que volem signar, el següent pas és autenticar-se amb TrustedX per utilitzar els recursos de les identitats de signatura.
Al clicar al botó 'Login TrustedX' l'usuari es redirigit als serveis de TrustedX, en aquest moment s'executen les accions definides al cas d´ús CU-04.



Il·lustració 30 - Vista accés a TrustedX

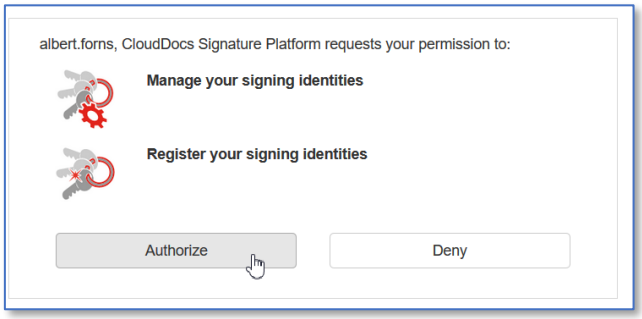
En un primer pas es sol·liciten les credencials d'usuari per tal de verificar-ne la identitat. Òbviament per autenticar-se a la plataforma de TrustedX ha estat necessari sol·licitar-ne l'alta.



Il·lustració 31 - Vista autenticació a TrustedX

Un cop autenticat es sol·licita l'autorització per a realitzar la gestió de les identitats de signatura i poder-ne registrar de noves; aquests recursos estan definits als abasts

urn:safelayer:eidas:sign:identity:manage i urn:safelayer:eidas:sign:identity:registre respectivament.

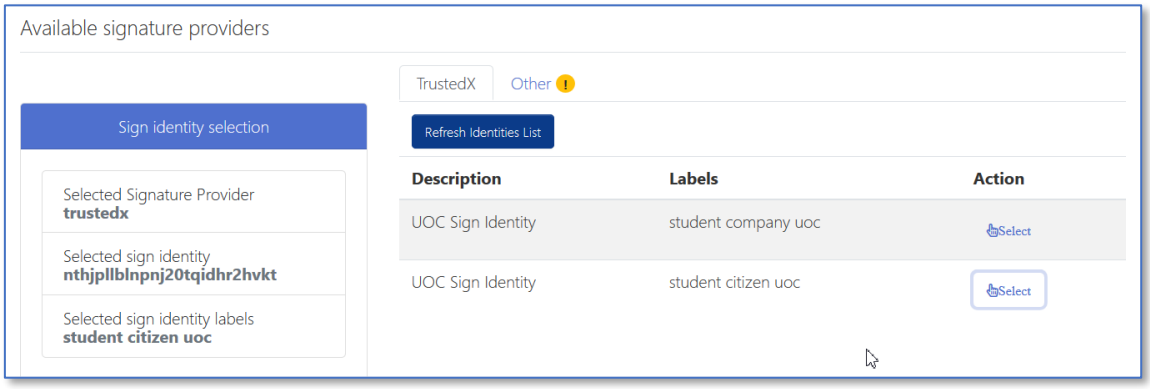


Il·lustració 32 - Vista autorització a la gestió d'identitats a TrustedX

Al finalitzar l'execució d'aquests passos, es guarda el token a la sessió d'usuari per no requerir aquests passos cada vegada que es vulgui treballar amb els recursos d'identitats.

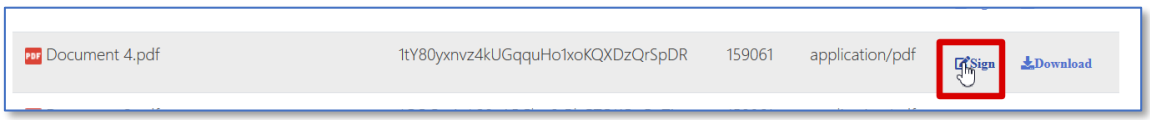
Arribats a aquest punt, ja tenim accés als recursos dels fitxers de Google Drive i als recursos d'identitats de TrustedX i ja només queda realitzar la signatura d'un document.

El pas previ a la signatura és la selecció de la identitat que s'utilitzarà, la selecció es guarda a la sessió d'usuari com a identitat per defecte.



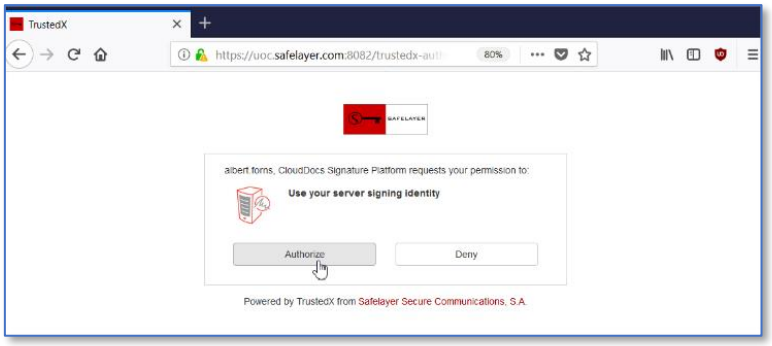
Il·lustració 33 - Vista llistat i selecció d'identitats

Per últim, quan es clica la icona 'Sign' relacionada amb el document s'executen les accions definides al cas d´ús CU-07.



Il·lustració 34 - Vista selecció document a signar

El token de TrustedX guardat a la sessió només és vàlid per a la gestió i registre d'identitats, en aquest punt es sol·licita una autorització d'un sol ús per a l'abast urn:safelayer:eidas:sign:identity:use:server que permet utilitzar les identitats per a realitzar signatures raw.



Il·lustració 35 - Vista autorització a l'ús d'una identitat per signar a TrustedX

Un cop autoritzada, la plataforma CloudDocs fa la crida a TrustedX per a realitzar la signatura, recupera la resposta, genera el fitxer PDF signat i finalment el puja el fitxer resultant a Google Drive.

Per a més informació del funcionament de la plataforma pot consultar la guia d'usuari annexada a aquesta memòria (CloudDocs_UserGuide.pdf).

8. Conclusions

Els constants canvis normatius en la legislació provoquen que el software requereixi de canvis i adaptacions de forma continuada; però al mateix temps obre les portes a nous productes i serveis, com és el cas de TrustedX de Safelayer utilitzat en aquest TFM i que n'és una peça fonamental. Aquest servei, juntament amb dos dels serveis d'emmagatzemament de fitxers al núvol més estesos entre els usuaris com són Google Drive i Dropbox han estat utilitzats en la plataforma creada per acabar oferint un servei afegit consistent en la signatura electrònica qualificada de documents PDF.

Els objectius marcats s'han complert amb èxit, ja que s'ha assolit la fita de crear una plataforma que permet signar documents en format PDF sense disposar ni dels fitxers ni dels certificats en local, utilitzant els recursos ubicats el núvol accessibles a través de diversos serveis.

En la definició inicial d'aquest TFM es van definir uns objectius bàsics per a dur a terme la idea principal dins del termini de que es disposava per a la realització d'aquest. Durant la realització del TFM es van poder afegir funcionalitats no incloses en la planificació inicial, com per exemple la integració amb Dropbox, ja que el calendari ho va permetre. Altres idees que van sorgir en la definició del pla de treball que finalment no es van afegir han estat incloses en l'apartat de treballs futurs.
En línies generals s'ha pogut seguir programa establert, tot i que hi ha hagut alguna tasca que ha causat bloqueigs puntuals en el desenvolupament degut a la inexperiència en l'ús d'algunes llibreries externes.

La seguretat ha estat un aspecte d'especial rellevància en aquest projecte. Com qualsevol plataforma web amb un mínim de seguretat s'ofereix sota el protocol HTTPS, però el punt a tenir en compte és la seguretat en el consum dels serveis utilitzats. Tots els accessos als endpoints dels serveis REST oferts també es realitzen per HTTPS i, a més, qualsevol accés i ús d'un recurs requereix sempre l'autorització de l'usuari autenticat als serveis i que és el propietari d'aquets recursos.

Pel que fa referència a la implementació, aquesta possiblement té alguns punts que es poden millorar, ja sigui el patró de disseny o l'eficiència d'alguns components; però cal tenir en compte que no tenia massa experiència prèvia amb el framework utilitzat i ha estat una bona oportunitat per adquirir nous coneixements.

8.1. Treballs futurs

L'aplicació resultant d'aquest TFM és senzilla per a poder-la considerar un producte final. Per tal de completar-la es podrien realitzar una sèrie de millores que es detallen a continuació:

- Millorar presentació i integracions amb els FFS

Implementar la funcionalitat per a poder paginar correctament els resultats dels fitxers obtinguts dels diferents FFS per a aquells casos que hi ha molts fitxers en un directori no es mostrin tots a la mateixa pàgina.

- Gestió d'accés als usuaris

Actualment l'aplicació realitza l'autenticació amb el servei d'identitats de Google. Seria interessant poder restringir l'accés únicament a usuaris autoritzats que siguin subscriptors del servei, això requeriria un registre d'aquests usuaris, restricció de l'accés al sistema, gestió de les subscripcions i integració amb una plataforma de pagament.

- Gestió de quotes

Lligat amb el punt anterior, resultaria interessant limitar les funcionalitats en funció del tipus de subscripció. Aquests limitacions podrien imposar-se en l'accés als diferents proveïdors d'emmagatzematge de fitxers o el nombre de signatures a realitzar durant una mensualitat.

- Configuracions personalitzades

Permetre seleccionar la identitat per defecte a l'usuari per no haver de seleccionar-la a cada accés o el FSS preferit per accedir-hi de forma automàtica quan accedeix a l'aplicació.

- Persistència de dades

Qualsevol de les tres funcionalitats anteriors requeririen disposar d'una base de dades. També es podrien emmagatzemar els històric de les accions realitzades pels usuaris per tal de poder-ho explotar posteriorment.

- Ampliar proveïdors de serveis

Integrar-se amb altres serveis d'emmagatzematge de fitxers que gaudeixin d'un nombre d'usuaris elevat com podrien ser OneDrive (Microsoft), Box, iCloud, etc. Al mateix temps també es podrien afegir nous eSigP.

- Verificar la signatura dels documents

L'eSigP de TrustedX disposa d'una funcionalitat per tal de validar les signatures dels documents.

- Múltiples signatures

Actualment l'aplicació només permet realitzar una signatura per document. Seria interessant poder realitzar múltiples signatures sobre un document i al mateix temps verificar que un document no s'intenta signar dues vegades amb el mateix certificat.

- Peticions i avisos

Realitzar peticions de signatura de documents a altres usuaris de la plataforma.

- Signatura en local

Poder signar en local documents allotjats al cloud. Aquesta funcionalitat s'allunyaria de la filosofia de l'aplicació que pretén que tot estigui al cloud, tot i que podria resultar interessant.

- Ampliar proveïdors d'identitat

L'aplicació utilitza com a proveïdor d'identitat els serveis de Google. Podrien utilitzar-se altres proveïdors com Linkedin, Facebook, Amazon, Microsoft, etc.

9. Glossari

En el aquest apartat es defineixen els termes i acrònims més rellevants utilitzats dins la memòria del TFM.

IdP: Proveïdor d'Identitat (*Identification Provider*)

AS: Servidor d'Autorització (*Authorization Service*)

FSS : Servei d'Emmagatzematge de Fitxers (*File Storage Service*)

eSigP: Proveïdor de Signatura electrònica (*Electronic Signature Provider*)

OAuth: és un estàndard obert per a l'autorització, que s'utilitza normalment com una forma perquè els usuaris d'Internet autoritzin llocs web o aplicacions per accedir a la seva informació en altres llocs web, però sense donar-los les contrasenyes.

OAuth2.0: La versió 2.0 proporciona fluxos d'autorització específica per a aplicacions web, aplicacions d'escriptori, telèfons mòbils i altres dispositius personals. [18]

Signatura electrònica avançada: Aquest tipus de signatura ha de complir els següents punts: [5]

- Estar vinculada al firmant de manera única.
- Permetre la identificació del firmant
- Haver estat creada utilitzat dades de creació de la signatura electrònica que el signant pugui utilitzar, amb un alt nivell de confiança, sota el seu control exclusiu.
- Ha d'estar estar vinculada amb les dades del signant de tal format que qualsevol modificació posterior dels mateixos sigui detectable.

10. Bibliografia

[1] [En línia]. Available: https://www.boe.es/doue/2014/257/L00073-00114.pdf. [Últim accés: Maig 2018].

[2] [En línia]. Available: https://blog.signaturit.com/es/eidas-nuevos-tiempos-para-la-firma-electronica-en-europa. [Últim accés: Maig 2018].

[3] [En línia]. Available: https://www.boe.es/buscar/act.php?id=BOE-A-2003-23399. [Últim accés: Maig 2018].

[4] [En línia]. Available: https://www.boe.es/buscar/doc.php?id=DOUE-L-2000-80059. [Últim accés: Maig 2018].

[5] [En línia]. Available: https://www.electronicid.eu/es/firma-electronica-avanzada/. [Últim accés: Maig 2018].

[6] [En línia]. Available: https://www.java.com/es/download/faq/java_webstart.xml. [Últim accés: Maig 2018].

[7] [En línia]. Available: http://openid.net/specs/openid-authentication-2_0.html. [Últim accés: Maig 2018].

[8] [En línia]. Available: https://es.wikipedia.org/wiki/OpenID. [Últim accés: Maig 2018].

[9] [En línia]. Available: http://openid.net/specs/openid-authentication-1_1.html. [Últim accés: Maig 2018].

[10] [En línia]. Available: http://openid.net/specs/openid-authentication-2_0.html. [Últim accés: Maig 2018].

[11] [En línia]. Available: http://openid.net/specs/openid-connect-core-1_0.html. [Últim accés: Maig 2018].

[12] [En línia]. Available: http://openid.net/connect/. [Últim accés: Maig 2018].

[13] [En línia]. Available: https://www.cryptomathic.com/products/authentication-signing/digital-signatures-faqs/what-type-of-authentication-can-be-used-for-remote-signing-according-to-eidas. [Últim accés: 2018 Maig].

[14] [En línia]. Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/40044784/Guidance%20on%20Levels%20of%20Assurance.docx?version=1&modificationDate=1488295895839&api=v2. [Últim accés: Maig 2018].

[15] [En línia]. Available: https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2. [Últim accés: Maig 2018].

[16] [En línia]. Available: http://www.bubblecode.net/en/2016/01/22/understanding-oauth2/. [Últim accés: Maig 2018].

[17] [En línia]. Available: https://www.pdfa.org/publication/iso-32000-1-pdf-1-7/. [Últim accés: Maig 2018].

[18] [En línia]. Available: https://oauth.net/2/. [Últim accés: Maig 2018].

11. Annexos

- CloudDocs_UserGuide.pdf: Guia d'usuari on es detallen els requisits per a poder treballar amb l'aplicació i les diferents funcionalitats implementades.

- Repositori GIT que conté el codi font de l'aplicació. Aquest està ubicat a https://bitbucket.org i es van proporcionar els accés necessaris al tutor.

- Aplicació web publicada a l'enllaç https://uoc.safelayer.com:9080/clouddocs/