Universitat Oberta de Catalunya

uoc.edu

# *Sistemes d'autenticació i autorització*

# *CloudDocs Signature Platform*

**Alumne: Albert Navarro Sánchez**
**Pla d'estudis:** *Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions*
**Àrea del Treball Final:** *TFM - Ad hoc*

**Consultor:** *Juan Carlos Fernández Jara*

**PRA:** *Víctor García Font*

31/12/2018

**FITXA DEL TREBALL FINAL**

| | |
|---|---|
| **Títol del treball:** | *Sistemes d'autenticació i autorització CloudDocs Signature Platform* |
| **Nom de l'autor:** | *Albert Navarro Sánchez* |
| **Nom del consultor/a:** | *Juan Carlos Fernández Jara* |
| **Nom del PRA:** | *Víctor García Font* |
| **Data de lliurament (mm/aaaa):** | *12/2018* |
| **Titulació o programa:** | *Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions* |
| **Àrea del Treball Final:** | TFM - Ad hoc |
| **Idioma del treball:** | *Català* |
| **Paraules clau** | *Signature, eIDAS, Cloud* |


**Resum del Treball:**

El projecte CloudDocs Signature Platform té com a finalitat l'estudi del reglament eIDAS i la generació de signatures electròniques. L'aplicació web resultant busca també l'eliminació dels requisits habituals a l'hora de la signatura com el de disposar d'un lector físic de certificats. Per assolir els objectius s'utilitzaran diversos serveis cloud com GoogleDrive o Dropbox per obtenir fitxers. D'altra banda per realitzar les signatures s'utilitzarà TrustedX per obtenir les identitats de signatura. Per donar validesa legal al procés de signatura s'estudia del reglament eIDAS per ajustar els processos de signatura per al seu compliment.

El projecte ha assolit l'objectiu principal d'obtenir una aplicació base que permetés estudiar com utilitzar els protocols d'autenticació com OAuth2, els servidors de recursos i un gestor d'identitats com TrustedX per tal d'ajustar-lo a la nova reglamentació eIDAS. L'opció de millorar i dotar d'un LoA superior a l'aplicació i l'evolució de les funcionalitats integrades dins l'aplicació deixa la porta oberta a estudiar les possibilitats d'aquest projecte més enllà d'una prova de concepte.

**Abstract:**

CloudDocs Signature Platform has the aim of study the eIDAS framework and electronic signature processes generation. The final web app searches to remove physical barriers from electronic signature actions such as smart card readers. In order to achieve the main goals we will use files cloud services as GoogleDrive or Dropbox and a identity cloud service called TrustedX. All workflows needed on the signature process will be supported by eIDAS framework

The project has achieved the main goal as the web app developed has allowed to study authentication protocols as OAuth2, resource serves and a identity manager (TrustedX) and how adapt them to eIDAS framework. Improving the LoA and the main functionalities from the web app we can achieve a application that can make a step forward and become something more as just a prove of concept.

# Índex

# 1. Introducció

## 1.1 Context i justificació del Treball

En una societat on moltes de les accions es duen a terme fàcilment de forma telemàtica trobem encara processos que trenquen amb aquesta filosofia. La signatura de documents electrònica n'és un d'ells. Signar un document electrònicament és encara una odissea en alguns casos i no tots els usuaris disposen sempre de les eines necessàries per dur-la a terme. Software específic, dispositius de lectura certificats, etc. són elements imprescindibles per a realitzar aquesta acció.

Per molts usuaris el fet de precisar d'aquests requisits comporta un rebuig a la utilització d'aquest mètode per signar els documents digitals. A l'estat espanyol, per exemple, tothom qui necessiti utilitzar el certificat electrònic del eDNI necessita sempre un lector que permeti llegir el certificat i identificar l'usuari. Usar certificats doncs, és una tasca gens fàcil i que no es mostra d'una manera accesible als usuaris.

La necessitat de disposar d'uns entorns específics per a la signatura de documents va en contra de la tendència actual del món tecnològic, on l'usuari gairebé pot fer totes les gestions a tot arreu i tan sols amb el seu dispositiu mòbil. Els usuaris gaudeixen d'una tecnologia que els ofereix facilitats i no impediments, per exemple, sols amb un usuari i contrasenya de Google és possible accedir a centenars d'aplicacions. Si necessiten compartir documents o accedir-hi des de múltiples localitzacions poden fer-ho amb GoogleDrive, DropBox, OneCloud, etc. Fins i tot els poden editar online. ¿Per què la signatura electrònica no disposa d'aquestes facilitats al cloud?

Aquest projecte busca trobar una solució que doni a l'usuari les mateixes facilitats per signar documents que les que disposa per accedir-hi. L'obstacle principal que es troba un usuari al signar electrònicament és la necessitat de tenir un dispositiu hardware que llegeixi el certificat, per tant, el primer pas és eliminar aquest requisit. Aplicant la lògica de tots els serveis actuals, la solució passa per allotjar al cloud el servei de custòdia de certificats i claus de l'usuari. Si els documents es signen al núvol, eliminem la principal barrera dels usuaris. En aquest projecte serà TrustedX Safelayer el servei que gestionarà la informació dels certificats a l'usuari i qui donarà el servei de claus per a poder signar els documents.

CloudDocs Signature Platform busca donar una solució completa a tot el procés de signatura al cloud. L'aplicació té com objectiu aglutinar els diferents Resource Servers que actualment existeixen al cloud com Google Drive o DropBox, encarregats de gestionar documents, i TrustedX, encarregat de proveir a l'usuari claus per a la signatura de documents. D'aquesta manera Cloud Docs oferirà a l'usuari un servei des del qual autenticar-se, accedir a fitxers i generar la signatura d'aquests disposant només d'una connexió a internet i un navegador web.

## 1.2 Objectius del Treball

La fita principal d'aquest projecte és el desenvolupament d'un aplicació que permeti la signatura electrònica de documents en un entorn cloud sense la necessitat de l'ús de perifèrics. Per tal d'assolir aquesta fita principal, s'hauran de complir aquestes fites secundàries durant el transcurs del projecte:

- Entendre els principals components del protocol d'autenticació OAuth2 així com dels fluxos per autenticar usuaris a través de múltiples plataformes.
- Dotar l'aplicació dels sistemes necessaris per a que sigui segura i no es posin en perill les dades dels usuaris.
- Estudiar el marc legal de les signatures electròniques per a assegurar que els documents signats per l'aplicació tenen validesa a la Unió Europea (UE)
- Dotar l'aplicació de la capacitat d'accedir i signar documents de diferents proveïdors de fitxers cloud com podrien ser Google Drive o DropBox. L'aplicació també haurà de tenir la capacitat d'incorporar fàcilment nous proveïdors en un futur.
- Estudiar la relació que tindrà l'usuari amb l'aplicació. Les funcionalitats de les quals disposi l'aplicació hauran de satisfer les necessitats de l'usuari.
- Comprendre els passos necessaris per a la signatura electrònica de documents així com els principals actors que hi intervenen.
- Desenvolupar la integració de l'aplicació amb el sistema extern de gestió de certificats i signatures TrustedX.
- Realitzar un estudi sobre les possibles millores de l'aplicació un cap assolit el primer prototip.

## 1.3 Enfocament i mètode seguit

La metodologia que seguirà el projecte per a l'assoliment de les fites marcades poden agrupar-se en diferents fases:

- Definició del projecte i del pla de treball: en aquesta etapa es busca definir l'abast del projecte així com els objectius principals, la metodologia, les tasques i la planificació per a dur-les a terme.
- Anàlisi del protocol OAuth2: aquesta fase ha de servir per a comprendre el protocol i els seus actors principals. Entendre el seu funcionament i realitzar la primera prova de concepte per autenticar usuaris a través de serveis de tercers es el principal objectiu.
- Estudi APIs GDrive i DropBox i elaboració de la integració amb l'aplicació: aquesta fase tindrà com objectiu estudiar la manera en que l'aplicació comunicarà amb els diferents proveïdors de fitxers per a mostrar la informació adient als usuaris.
- Anàlisi de requisits casos d'ús i fluxos de l'aplicació: aquesta etapa tindrà com a resultat un anàlisi de requisits funcionals que ha de complir l'aplicació per a que sigui capaç de donar solució els problemes plantejats.

- Estudi de la llei eIDAS: la llei eIDAS estableix una sèrie de requisits per a que una signatura sigui vàlida arreu la UE, per aquest motiu el seu estudi i aplicació al projecte és bàsica per dotar d'un marc legal la solució proposada per CloudDocs Signature Platform.
- Desenvolupament aplicació: la fase de desenvolupament de l'aplicació es transversal durant tot el projecte i ha de donar com a resultat un prototip que compleixi amb els requisits funcionals. Aquesta fase transversal té les seves pròpies fites:
    - Desenvolupament de la interfície d'usuari de l'aplicació web que permetrà a l'usuari autenticar amb els diferents serveis d'autenticació i gestionar els fitxers de seu cloud.
    - Incorporació de servei de signatura electrònica TrustedX eIDAS Platform de Safelayer: es realitzarà al integració de TrustedX a l'aplicació per a poder realitzar gestionar els certificats electrònics que permetran la signatura de documents al Cloud.
    - Signatura electrònica de documents: es realitzarà la connexió definitiva entre els proveïdors de fitxers i el proveïdor de certificats per a realitzar la signatura electrònica dels documents.
- Test i verificació de funcionalitats: en aquesta fase es realitzaran les proves funcionals de l'aplicació i es verificarà que compleixen amb els requisits detallats al projecte. També s'analitzaran els possibles *bugs* que puguin sorgir.
- Anàlisi de resultats i millores: l'última fase del projecte constarà de l'anàlisi dels resultats i la conseqüent proposta de millores de l'aplicació així com de les conclusions finals del projecte.

## 1.4 Planificació del Treball

*Definició del projecte i del pla de treball*

Aquesta tasca implica l'estudi de l'estat de l'art i el context en el qual s'emmarca el projecte i l'elaboració del pla de treball que permetrà arribar a l'objectiu principal. El resultat final és l'entregable PAC1.

*Anàlisi del protocol OAuth2*

S'elaboren esquemes amb el flux del protocol i s'identifiquen els actors que hi intervenen.

*Estudi APIs GDrive i DropBox i integració amb l'aplicació*

Es descriu com es poden utilitzar les APIs d'aquests serveis per a recollir la informació que vol l'usuari des d'una sola plataforma.

*Anàlisi de requisits i casos d'ús de l'aplicació*

Es descriuen tots els casos d'ús de l'aplicació i s'elabora un anàlisi de requisits que s'han d'assolir per a complir amb les necessitats dels usuaris de l'aplicació. En aquesta tasca s'elabora l'entregable de la PAC2 que recull els punts 2-4.

*Estudi de la llei eIDAS*

S'estudia el marc legal de la llei eIDAS i se'n descriuen els punts elementals que ha de tenir una signatura electrònica per a que tingui validesa a la UE. un cop identificats els requisits es justificarà la validesa de les signatures emeses per l'aplicació.

*Desenvolupament aplicació*

S'elabora l'arquitectura de l'aplicació i es defineixen les parts que la componen. Un cop definides s'inicia el desenvolupament de les parts implicades (Integració amb GDrive y DropBox amb TrustedX). Aquesta tasca és transversal i es duu a terme durant tot el projecte. Aquesta tasca anirà recollida juntament amb l'estudi de la llei eIDAS a l'entregable associat a la PAC3.

*Test i verificació de funcionalitats*

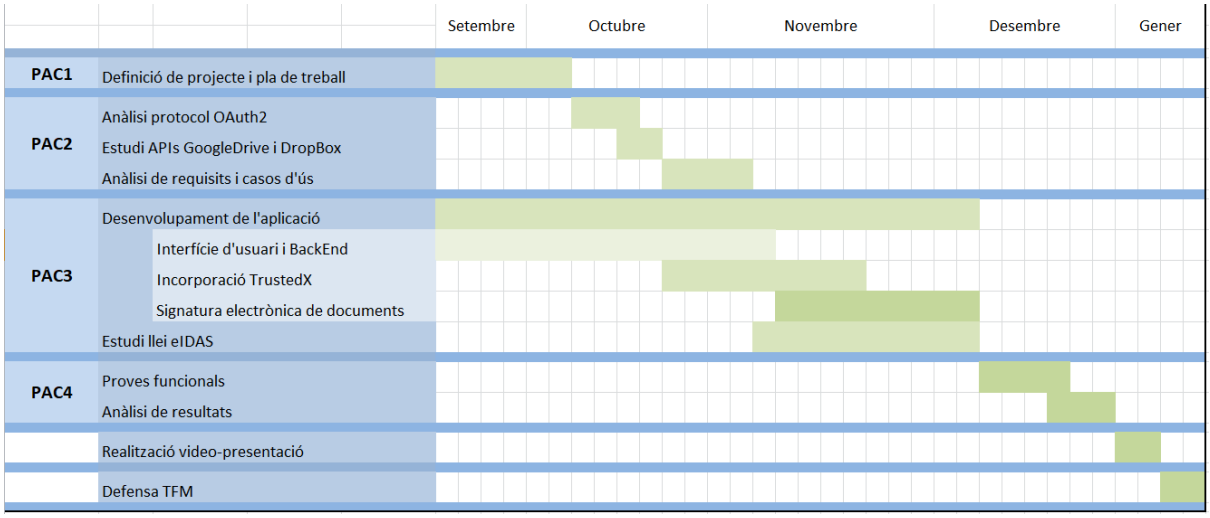
Un cop desenvolupada l'aplicació es realitzen les proves funcionals recollides a la PAC2 i se'n verificarà el correcte funcionament.

*Anàlisi de resultats i millores*

S'analitzen els resultats de les proves funcionals i se n'extreuen les conclusions d'aquestes. Recollides les conclusions es proposen treballs futurs per a la millora del projecte. S'agrupen tots els entregables i s'entrega la PAC4 amb la versió final de la memòria.

*Realització de la video-presentació*

Es realitza una presentació del projecte utilitzant dispositives i una veu en off.




## 1.5 Breu sumari de productes obtinguts

PAC1: es tracta del pla de treball, en el qual es defineixen objectius i s'elabora la planificació del treball.

PAC2: aquesta entrega recollirà la informació de les fases Anàlisi del protocol OAuth2, Estudi APIs GDrive i DropBox i integració amb l'aplicació i Anàlisi de requisits i casos d'ús de l'aplicació.

PAC3: es tracta de l'última part de l'estudi on s'estudiarà la llei eIDAS i es finalitzarà el desenvolupament de l'aplicació.

PAC4: es fa un recull de les entregues anteriors afegint els resultats de les proves funcionals i les conclusions del treball.

PAC5: es realitza la vídeo-presentació del treball.

# 2. Estat de l'art

Internet ha esdevingut una de les eines principals de la societat amb l'ajuda de la telefonia mòbil i els serveis allotjats al Cloud. De la unió d'aquests tres conceptes; Social, Mòbil i Cloud, obtenim SoMoClo que engloba els tres pilars de la computació moderna.

D'aquests termes se'n deriven múltiples reptes relacionats amb la seguretat, la confiança i la gestió de la identitat dels usuaris. Aquests conceptes evolucionen i es desenvolupen en harmonia amb les necessitats del moment i a la velocitat que ho fa internet. Una regularització de la xarxa ajuda, però aquesta ha d'anar acompanyada de la complicitat i la involucració dels agents regulats. Probablement aquesta sigui la causa principal del poc èxit de la Directiva 1999/93/EC, i aquest ha de ser l'objectiu del nou reglament eIDAS.

L'evolució de la gestió de les identitats, des d'una contrasenya fins a una targeta intel·ligent PKI com els ePassports o els citizensID demostra la rapidesa en que s'actualitzen els mètodes de gestió de la identitat. Per aquets motiu el nou reglament eIDAS no parla de mecanismes en si, sinó de nivells de seguretat. EIDAS posa el focus en la identificació electrònica eID d'on neixen els Trust Services o Identity Services. D'altra banda els elements bàsics dels quals es desenvolupen tots els serveis de confiança són "electronic Authentication" i "electronic Signature". Ajuntant els conceptes esmentats obtenim "electronic IDentification, Authentication and Signature", amb acrònim eIDAS.

Els diferents elements de SoMoClo juguen un paper determinant dins el món tecnològic.

*Social:* les principals companyies de les xarxes socials com Google o Facebook han esdevingut en proveïdors d'identitat (IdP). Només amb Facebook, amb 1300 milions d'usuaris, es poden accedir a milers d'aplicacions realitzant una sola acció de login (sistema de Single Sign-On).

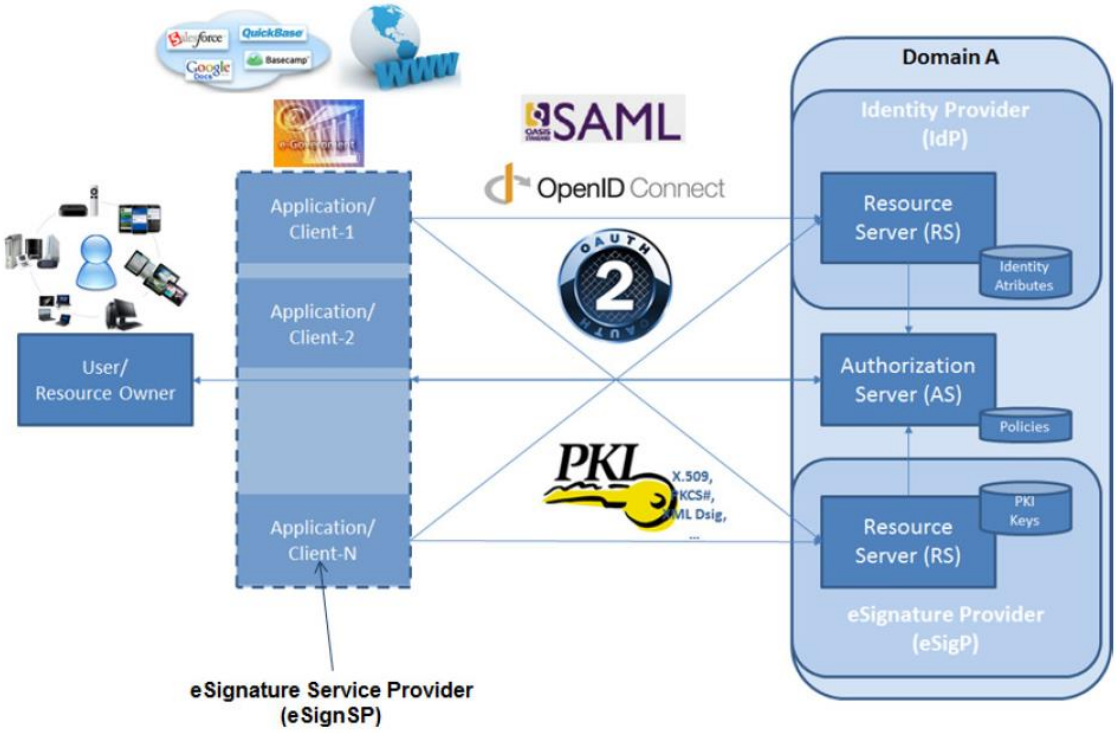
*Mòbil:* els dispositius mòbils s'han convertit en l'eina principal de connexió amb la societat digital. Gràcies a les funcionalitats d'identificació que disposen com la lectura dactilar, reconeixement d'imatge i veu podrien aportar quantiosament a l'àmbit de la identificació electrònica, authentication and signature (eIDAS) o fins i tot convertir-se en el eID per excel·lència.

*Cloud:* el Cloud, és imparable. Les organitzacions demanen compatibilitzar els sistemes existents on-premise amb noves aplicacions i serveis Cloud i alhora gestionar de forma unificada les identitats dels seus usuaris. Per cobrir aquesta demanda els proveïdors dels serveis Cloud ofereixen a les organitzacions Federacions d'Entitats. D'aquesta forma els repositoris d'identitat s'allotgen dins les instal·lacions de l'organització i els usuaris s'autentiquen sempre internament federant la seva identitat amb el proveïdor Cloud el qual rep la informació mínima necessària per realitzar les

seves funcions. Dins dels proveïdors de servei Cloud també trobem gestors d'identitat, o IDaaS (Identity as a Service) que ofereixen funcionalitats de gestió d'identitats basades en PKI.

Els vectors Social, Mobile and Cloud poden ajudar a desplegar i accelerar l'èxit de la nova proposta del reglament eIDAS. Partint d'aquesta base Safelayer Secure Communications proposa un esquema que ha de permetre cobrir els objectius eIDAS a nivell europeu pel que fa a electronic Identificatoin, Authentication, and Signature. La proposta es basa en serveis, protocols i arquitectures ja existent.

## 2.1 Arquitectura base




L'arquitectura implementa un model user-centric en el qual els usuaris poden o bé autoritzar l'entrega de la seva identitat a d'altres aplicacions o en altre cas que el proveïdor d'entitats (IdP) defineixi certes polítiques d'autorització que l'usuari ha d'acceptar explícitament. El model proposat és la combinació d'un Identity Provider (IdP) amb un Authorization Server (AS) junt amb les entitats Se Service Provider i Relying Party (les quals només difereixen pel nom) i un usuari a compartir entre ambdós recursos (IdP i AS).

## 2.2 Identity Provider (IdP)

Un Identity Provider és una entitat amb l'autoritat d'emetre informació relacionada amb la identitat d'un sistema. S'encarrega de donar la informació necessària a tots aquells proveïdors de serveis que requereixin confirmar la identitat d'un usuari com per exemple atributs d'identitat, autenticació, SSO i de Federació. En el cas presentat

també incorpora la funcionalitat addicional pròpia del model OAuth, un Resource Server (RS) que relaciona conjunts d'atributs d'identitat de l'usuari en "scopes" del propi model. Els Relying Parties poden sol·licitat autorització a l'usuari per accedir a aquests scopes a través del servidor d'autenticació.

### 2.3 Resource Servers (RS)

Un Resource Server és l'encarregat de gestionar l'accés als recursos d'un sistema. Un cop una aplicació ha obtingut una clau d'accés (token) per part del servidor d'autorització aquesta pot fer peticions al RS. El RS haurà de verificar el token amb el AS i un cop validada cedeix el recurs demandat per l'usuari.

### 2.4 eSignature Provider (eSigP)

En la seva base aquest component és un RS especialitzat en identitats PKI. Concretament en claus i certificats PKI per a ús electrònic. En aquest cas el RS delega les tasques d'autorització al AS que atorga l'autenticació en base a la informació de l 'IdP. Així doncs per accedir a un atribut PKI es requereix el mateix circuit que per qualsevol altre atribut que es pugui obtenir d'un altre RS.

### 2.5 Relying Parties i Aplicacions

Una relying Party (RP) és un component client que accedeix a recursos d'un RS controlat per un AS en nom d'un usuari. Dins l'esquema proposat, un cop autenticat l'usuari i donat el seu consentiment les RPs poden accedir a la informació d'identitat composta per atributs que ja poden ser comuns o de PKI. En el cas concret de CloudDocs Signature Platform trobem que l'aplicació ha d'accedir d'una banda a un RS d'arxius PDFs com GoogleDrive o DropBox i a un RS de certificats que en el nostre cas serà TrustedX

### 2.6 Protocols

Els protocols en els quals es basa el framework proposat són estàndards coneguts i usats àmpliament a internet. Aquests protocols sustenten els serveis i funcionalitats dels components IdP i eSigP. Pel que fa a l'autenticació es proposen els protocols OpenID Connect 1.0 i el SAML 2.0. El primer basat en OAuth i el segon dona suport a les tasques de SSO per connectar amb sistemes empresarials. Aquests protocols permeten estandarditzar els serveis i funcionalitats pròpies d'un IdP. En referència a l'autorització de l'usuari per l'accés a dades per part d'altres aplicacions es planteja l'ús d'OAuth2. Aquest protocol permet de forma fàcil accedir a recursos des de qualsevol infraestructura web que treballi amb HTTP sense deixar de banda la privacitats dels usuaris.

### 2.7 Serveis

Dels serveis que ha d'oferir el framework proposat per SafeLayer en destaquem els següents:

- Electronic identification: permeten registrar, emetre i gestionar el cicle de vida dels eIDs de qualsevol tipus així com associar diferents atributs d'identitat que defineixen a un usuari a aquests eIDs.
- Authentication: permeten verificar les identitats electròniques en base a les credencials eID dels usuaris fent us de protocols segurs.
- Authorization: des de la perspectiva user-centric de la gestió d'identitat, el framework ha de permetre l'usuari cedir de forma explícita l'entrega d'atributs d'identitat a un proveïdor de serveis (SP) o Relying Party (RP) amb la que interactuï.
- Single Sign-On: permet als usuaris i aplicacions un inici únic de sessió dins d'una federació de confiança. Amb una sola acció de login l'usuari aconsegueix accedir a múltiples aplicacions i serveis sense tornar a autenticar-se.
- Electronic Signature: el framework pretén formalitzar aquests servei com una funció a la qual s'aplica una credencial per produir una signatura electrònica avançada en els termes definits a la clàusula (11) de l'article 3 de la nova regulació eIDAS.

# 3.Disseny de l'aplicació

CloudDocs Signature platform és una prova de concepte del framework proposat per SafeLayer. La identificació de les diferents parts així com dels protocols i serveis Cloud utilitzats pel desenvolupament del projecte responen a les entitat requerides pel framework.

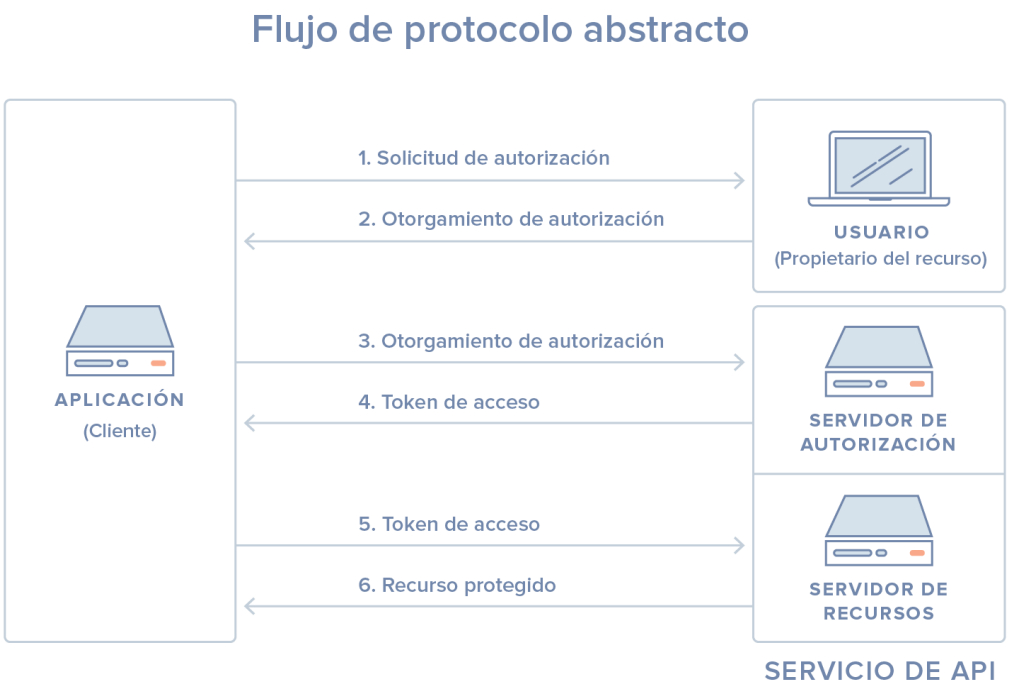
## 3.1 Protocol oAuth2

És un protocol estandarditzat que permet l'autorització a les aplicacions obtenir accés limitat a dades d'usuari  través d'HTTP com Facebook, Google, entre d'altres. Delega l'autenticació de l'usuari al servei d'autenticació que allotja el compte de l'usuari i autoritza a aplicacions de tercers a utilitzar la informació del compte en qüestió. El protocol OAuth2 defineix quatre rols:

*Propietari del recurs:* el propietari és l'usuari que dóna l'autorització a una aplicació, en el nostre cas CloudDocs SP, per accedir al seu compte. L'accés de l'aplicació es limita a les àrees permeses per l'usuari. Per exemple, un usuari pot decidir si dóna permisos d'escriptura, o només de lectura sobre uns arxius.

*Servidor de recursos i d'autorització:* el servidor de recursos allotja els comptes dels usuaris i el servidor d'autorització verifica les identitats de l'usuari. Un cop verificada la identitat genera els tokens necessaris pel consum de la informació.

*Client:* el client és l'aplicació que vol accedir al compte de l'usuari. Abans de fer-ho, però ha de rebre l'autorització per part de l'usuari.




Aquests quatre rols interactuen de la següent manera:

1. L'aplicació sol·licita autorització per accedir als recursos del servei de l'usuari.
2. En cas de que l'usuari accepti la sol·licitud l'aplicació rep una autorització.
3. L'aplicació sol·licita al servidor d'autorització un token d'accés presentant l'autenticació de la seva identitat (aplicació) i l'autorització donada al punt 2.
4. Si la identitat de l'aplicació és correcte i l'autorització vàlida el servidor d'autorització emet un token d'accés i l'autorització finalitza.
5. L'aplicació sol·licita el recurs al servidor de recursos presentant el token per autenticar-se.
6. Si el token es vàlid, el servidor de recursos retorna el recurs a l'Aplicació.

Abans però de que l'aplicació pugui sol·licitar les autoritzacions s'ha de registrar l'aplicació com a servei apte per treballar amb el servei web demandat per l'aplicació. La informació requerida és:

- Nom de l'aplicació
- Portal web de l'aplicació

- Redirect URI o Callback URL (és on el servei reorientarà l'usuari un cop autoritzada, o denegada, la sol·licitud.

*Identificador i secret del client*

Un cop registrada l'aplicació el servei web emet les credencials que tindrà l'aplicació en forma d'un identificador i d'un secret. L'identificador (ID) és una cadena pública que utilitza l'API del servei per identificar l'aplicació i generar les URLs d'autorització que usen els usuaris. Un cop l'aplicació sol·licita l0accés al compte de l'usuari el secret del client s'utilitza per autenticar la identitat de l'aplicació que està consumint l'API. A diferència de l'identificador, el secret és, com bé diu el nom, secret i no s'ha de fer públic.

## 3.2 IdPs i AS: Google - DropBox - TrustedX

Els Identity Providers utilitzats a CloudDocs Signature Platform corresponen amb els oferts pels dos serveis principals d'emmagatzematge d'arxius, Google i DropBox. Aquests dos serveis hauran de suplir les tasques d'autenticació dels usuaris i d'atorgar a l'aplicació les autoritzacions necessàries per a recuperar els recursos necessàries per al correcte funcionament de l'aplicació.
El servei de certificats TrustedX també disposa d'un IdP propi per autenticar els usuaris. Tot i que TrustedX ofereix la possibilitat de federar els usuaris de les aplicacions de Google i TrustedX s'opta per utilitzar els IdPs de manera separada per la simplicitat del projecte.

## 3.3 Resource Servers

L'aplicació CloudDocs Signature Platform es nodreix de dos tipus de Resource servers. D'una banda disposem dels RS que disposen la informació relacionada amb la gestió d'arxius i de l'altra el RS que disposa de la informació relacionada amb els certificats. Tot i que la gran majoria de RS implementen mètodes RestFull per accedir a la informació que allotgen és habitual que també disposin l'opció d'utilitzar llibreries específiques per consultar els recursos.

*Mètodes RestFull*

Els avantatges que aporta aquest mètode per consumir recursos son diversos:

- No requereix de programació ja que es poden consumir els recursos mitjançant crides HTTP des d'un navegador.
- La gran majoria utilitzen el mateix format a l'hora de retornar recursos. Un dels formats més estesos és el JSON.
- És State-less, per tant no s'emmagatzema cap informació de sessió.

- No requereix de contractes com el protocol SOAP.

Tots els serveis que s'utilitzen en aquest projecte disposen d'interfícies REST per obtenir els diferents recursos. Per exemple, per obtenir la llista de fitxers d'un usuari a Google Drive i DropBox :

*Google Drive*

```
GET https://www.googleapis.com/drive/v3/files
{
  "kind": "drive#fileList",
  "nextPageToken": string,
  "incompleteSearch": boolean,
  "files": [
    files Resource
  ]
}
```

*DropBox*

```
https://api.dropboxapi.com/2/file_requests/list
{
    "file_requests": [
        {
            "id": "oaCAVmEyrqYnkZX9955Y",
            "url":
"https://www.dropbox.com/request/oaCAVmEyrqYnkZX9955Y",
            "title": "Homework submission",
            "created": "2015-10-05T17:00:00Z",
            "is_open": true,
            "file_count": 3,
            "destination": "/File Requests/Homework",
            "deadline": {
                "deadline": "2020-10-12T17:00:00Z",
                "allow_late_uploads": {
                    ".tag": "seven_days"
                }
            }
        }
    ]
}
```

Per llistar la informació d'un usuari a TrustedX, per exemple faríem la crida:

```
GET /trustedx-resources/openid/v1/users/me
Host: trustedx.demo.com:8082
Authorization: Bearer a2b4...6daf

{
    "sub" : "john.doe",
    "domain" : "example.com",
    "username" : "john.doe",
    [ … ]
    "amr" : [ "urn:oasis:...:am:password",
"urn:oasis:...:am:OTP" ],
    "external_info" : {
        "my.social.net" : {
            "sub" : "817197465059411",
            "name" : "J. Doe",
            "email" : "jdoe@mymail.com"
        }
    },
    "authn_details" : {
        "directSso" : "false",
        "ipAddress" : "192.168.7.28",
        ...
    }
}
```

*Llibreries específiques*

Tot i la facilitat que presenta la crida d'aquests mètodes utilitzant qualsevol navegador pels serveis de Google Drive i DropBox s'utilitzaran llibreries específiques de cada servei. TrustedX en aquets cas no disposa de llibreries, per tant es faran les crides via HTTP. Aquestes llibreries ofereixen una capa per sobre del nivell HTTP i donen facilitat a l'hora d'incorporar els serveis dins de codi d'alt nivell. Disposant de les classes definides es poden accedir a les dades necessàries de forma més ordenada. Utilitzant llibreries Java l'acció de llistar fitxers quedaria:

*Google Drive*

```
final NetHttpTransport HTTP_TRANSPORT =
GoogleNetHttpTransport.newTrustedTransport();
Drive service = new Drive.Builder(HTTP_TRANSPORT, JSON_FACTORY,
getCredentials(HTTP_TRANSPORT))
            .setApplicationName(APPLICATION_NAME)
            .build();

// Print the names and IDs for up to 10 files.
FileList result = service.files().list()
            .setPageSize(10)
            .setFields("nextPageToken, files(id, name)")
            .execute();
List<File> files = result.getFiles();
```

*DropBox*

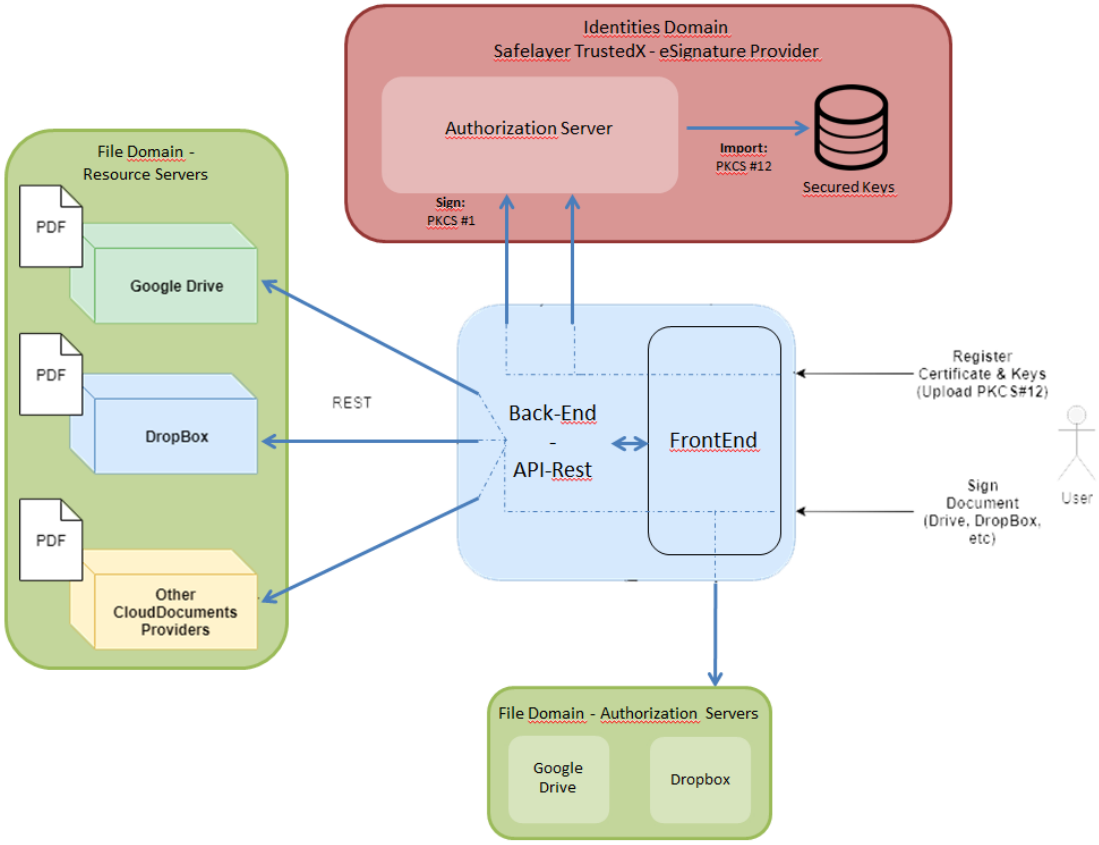
```
DbxRequestConfig config = new DbxRequestConfig("dropbox/java-tutorial",
"en_US");
DbxClientV2 client = new DbxClientV2(config, ACCESS_TOKEN);

// Get current account info
FullAccount account = client.users().getCurrentAccount();
System.out.println(account.getName().getDisplayName());

// Get files and folder metadata from Dropbox root directory
ListFolderResult result = client.files().listFolder("");
```

## 3.4 Arquitectura final

Identificades les parts del frameworks proposat per Safelayer i després d'enumerar com encaixaria cada element de CloudDocs Signature Platform l'arquitectura de l'aplicació seguiria el següent esquema. L'especificació interna de l'aplicació quedarà detallada durant els capítols següents. A l'esquema podem identificar els diferents elements l' IdP de Google i els RS de documents i certificats. Aquests elements queden units per l'aplicació principal que accedeix a sota demanda a tots els serveis.



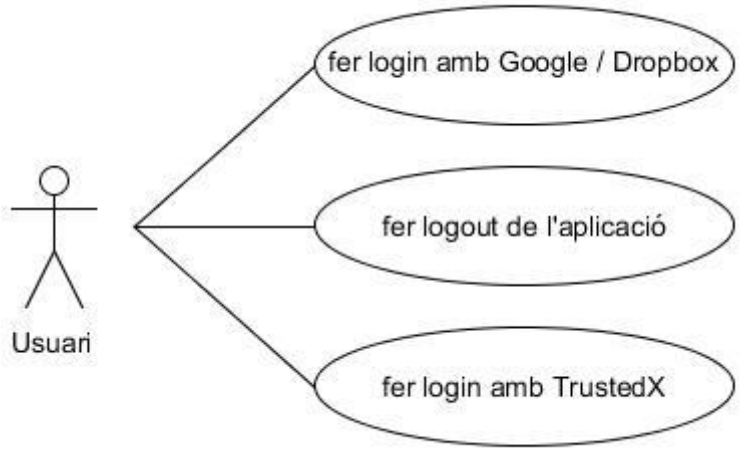

**Arquitectura CloudDocs Signature Platform**

## 3.5 Casos d'ús

En aquest apartat definim totes aquelles accions que un usuari ha de poder realitzar amb l'aplicació resultant. Les accions s'han dividit segons l'àmbit en el qual opera l'usuari.

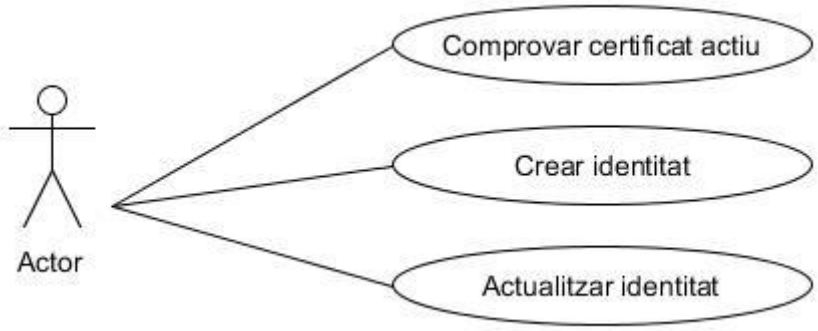
*Operacions amb IdP – Login*

- L'usuari ha de poder fer login amb Google o Dropbox
- L'usuari ha de poder fer logout
- L'usuari ha de fer Login a RS de certificats, però hauria de fer-ho un cop ha estat autenticat un dels RS de documents.



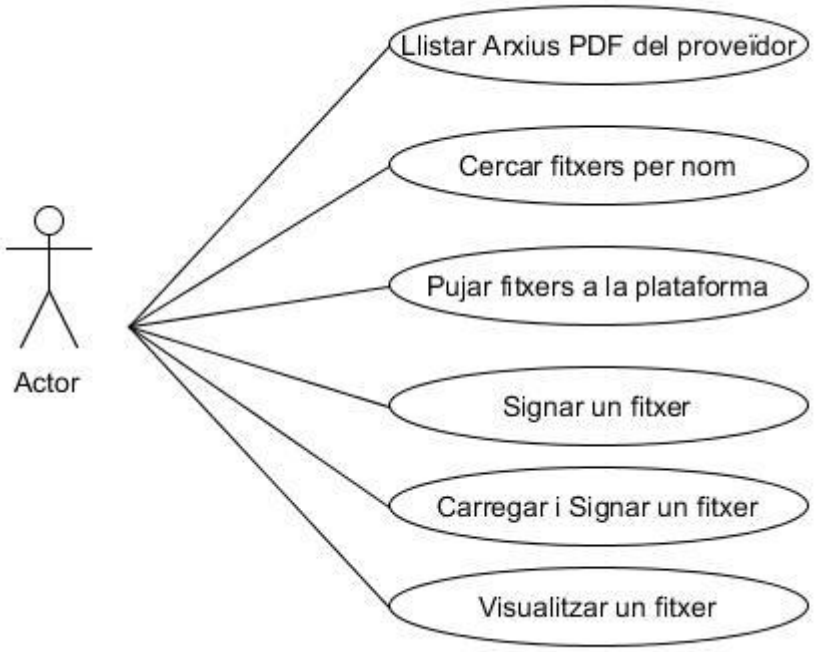

*Gestió de Certificats*

- L'usuari pot accedir i comprovar que si té, o no, un certificat al Resource server.
- L'usuari pot pujar una nova identitat. Si ja n'existeix una, es substitueix.
- L'usuari pot signar un document sempre i quan tingui un certificat al Resource server.




*Operacions amb documents*

- Llistar documents del RS. Únicament es llistaran arxius PDF.
- L'usuari pot realitzar cerques per nom de fitxer o indicar quina quantitat de resultats vol rebre
- L'usuari podrà pujar arxius a la plataforma on s'ha autenticat
- L'usuari pot signar els documents o pujar-ne un de nou i signar-lo a la mateixa acció
- L'usuari pot visualitzar un document abans de signar-lo



# Marc Legal

## TrustedX i eIDAS

TrustedX és una plataforma de serveis web per a la gestió de processos de signatura electrònica. Dins aquests processos inclou, entre d'altres, un repositori d'identitats i la pròpia generació de les signatures electròniques. El disseny del servei i les seves mesures de seguretat fan que encaixi dins de la definició de Dispositiu de Signatura Qualificat de la normativa eIDAS.

L'Art.29 del *REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE* conclou que els dispositius qualificats per a la creació de signatures han de complir els requisits establerts a l'Annex II de la mateixa normativa.

Requisits:

*1. Los dispositivos cualificados de creación de firma electrónica garantizarán como mínimo, por medios técnicos y de procedimiento adecuados, que:*

*a) esté garantizada razonablemente la confidencialidad de los datos de creación de firma electrónica utilizados para la creación de firmas electrónicas;*

En el moment de realitzar la signatura TrustedX aplica un LoA nivell alt per tal d'assegurar que només el propietari de la identitat de la signatura pot conèixer els detalls d'aquesta i utilitzar-la en processos de signatura.

*b) los datos de creación de firma electrónica utilizados para la creación de firma electrónica solo puedan aparecer una vez en la práctica;*

TrustedX només activa el servei de signatura en base a un token identificatiu que activa el procés. Un cop utilitzat aquest token en un procés de signatura, aquest queda desactivat i no pot ser utilitzat en cap altre procés de signatura.

*c) exista la seguridad razonable de que los datos de creación de firma electrónica utilizados para la creación de firma electrónica no pueden ser hallados por deducción y de que la firma está protegida con seguridad contra la falsificación mediante la tecnología disponible en el momento;*

TrustedX utilitza mètodes d'autenticació avançats per tal d'assegurar que només el propietari d'una identitat pot utilitzar-la.

*d) los datos de creación de la firma electrónica utilizados para la creación de firma electrónica puedan ser protegidos por el firmante legítimo de forma fiable frente a su utilización por otros.*

L'AuthServer, per poder activar la clau i poder identificar inequívocament l'usuari que les requereix pot demanar unes altres credencials per autoritzar operacions concretes. En aquest punt TrustedX sol·licita de manera expressa les credencials de l'usuari cada cop que s'han de realitzar operacions relacionades processos de signatura.

*2. Los dispositivos cualificados de creación de firmas electrónicas no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes de firmar.*

TrustedX disposa de dos mètodes per  la signatura de documents:

- Creació del Hash a signar i de la signatura al servidor: en aquest flux l'aplicació que utilitza TrustedX genera el hash que ha de signat al servidor passant-hi el document. Un cop obtingut el hash l'aplicació requereix a TrustedX que el signi.

- Creació de signatura al servidor: en cas l'aplicació genera el hash a signar pels seus propis mitjans i el servidor de TrustedX només en genera la signatura

En ambdós casos l'aplicació insereix la signatura final dins el document, per tant, en cas de que 1) en el cas 1 TrustedX generés un hash a partir de dades modificades o 2) TrustedX generés una signatura en base a un hash alterat el document resultant no podria ser validat doncs la verificació de la signatura seria errònia.

*3. La generación o la gestión de los datos de creación de la firma electrónica en nombre del firmante solo podrán correr a cargo de un prestador cualificado de servicios de confianza.*

Les operacions que realitza TrustedX durant el procés de signatura es realitzen íntegrament dins la pròpia aplicació, per tant, la identitat no és accedida per tercers.

*4. Sin perjuicio de la letra d) del punto 1, los prestadores cualificados de servicios de confianza que gestionen los datos de creación de firma electrónica en nombre del firmante podrán duplicar los datos de creación de firma únicamente con objeto de efectuar una copia de seguridad de los citados datos siempre que se cumplan los siguientes requisitos:*

*a) la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales;*

*b) el número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio.*

En aquest cas es pressuposa que la gestió de les identitats per part de TrustedX compleixen amb els requeriments d'aquest punt.

## CloudDocs Signature Platform: solució ideal

Per la signatura de documents l'aplicació utilitza els serveis de TrustedX. Aplicant els fluxos requerits per la normativa eIDAS el servei de CloudDocs SP hauria de gestionar les identitats i els processos de signatura de la següent manera:

*Certificats:*

El flux que s'haurien de seguir per tal de generar una identitat vàlida per realitzar signatures electròniques, per tal de complir la normativa hauria de ser:

1. L'aplicació demana generar la seva identitat del proveïdor d'identitats
2. TrustedX genera les claus (pública i privada) i la clau privada queda sota la seva custodia.
3. TrustedX demana un certificat per la clau generada a una CA Qualificada
4. TrustedX associa la clau protegida amb el certificat qualificat

Per la generació de la identitat TrustedX demana una autenticació a l'IdP amb LoA de nivell alt per tal de poder demostrar que l'usuari que genera el certificat és realment qui diu ser.

*Procés de signatura:*

El procés de signatura que hauria de seguir CloudDocs hauria de ser el següent:

1. CloudDocs demana signar un document:
    1. Es demana autorització a l'AuthServer indicant quina identitat s'utilitzarà per la signatura. El servidor autoritza l'usuari un cop garantida la seva identitat. En aquest punt l'AuthServer pot demanar d'altres credencials per a la verificació de l'usuari.
2. Rebuda l'autorització de TrustedX:
    1. Es genera el hash del document a signar. A TrustedX o a la pròpia aplicació.
    2. Es genera la signatura a TrustedX en base al hash generat.

## CloudDocs Signature Platform: solució proposada a la demo

L'aplicació resultant d'aquest projecte és una prova de concepte del flux presentat a l'apartat anterior. Per tal de poder fer aquesta demostració s'han simplificat els següents punts:

*Certificats:*

A la demo resultant l'usuari no genera un certificat qualificat amb TrustedX. Per tal de disposar d'un certificat demo l'usuari és capaç de pujar certificats *self-signed* a l'aplicació i generar les identitats a partir d'aquests.

El no precisar d'una entitat certificadora qualificada permet que TrustedX pugui rebaixar el nivell de LoA per a realització d'aquest procés identificant l'usuari només amb usuari i password.

*Procés de signatura:*

Pel que fa al procés de signatura els passos a seguir per part de CloudDocs no difereixen de la solució ideal. No obstant, en aquesta demo és TrustedX qui ha rebaixat el nivell d'exigència per a la realització de la signatura. A la demo el procés de signatura de TrustedX no requereix un LoA de nivell alt, ni un certificat qualificat. En un suposat cas de que la demo fos realment un producte definitiu s'hauria d'elevar el nivell de configuració de TrustedX per tal de pujar el LoA.

Aquest canvi en el nivell de LoA provoca que les signatures resultants de la demo de CloudDocs no siguin signatures qualificades, doncs cap CA ha verificat la identitat del certificat. Tot i així, les signatures generades per la demo compleixen amb els requisits d'una signatura avançada definits a l'Article 26 ja que:

1. La identitat està vinculada a un sol firmant
2. Es permet la identificació del firmant
3. Les signatures són creades amb certificat que el firmant pot utilitzar
4. Permet verificar la integritat del document signat fent possible la detecció de qualsevol modificació

# Definició de l'aplicació

## Arquitectura

CloudDocs Signature Platform és una aplicació web que permet fer login amb diversos IdPs i consumir recursos d'aquests com documents de Google Drive, DropBox... o identitats i signatures digitals de TrustedX.

L'arquitectura escollida pel desenvolupament de l'aplicació la separació de la web en una plana principal, Front End, que gestiona les sessions als diferents Resource Servers i permet comunicar amb el BackEnd, encarregat de gestionar totes les demandes de l'usuari cap als diferents servidors.

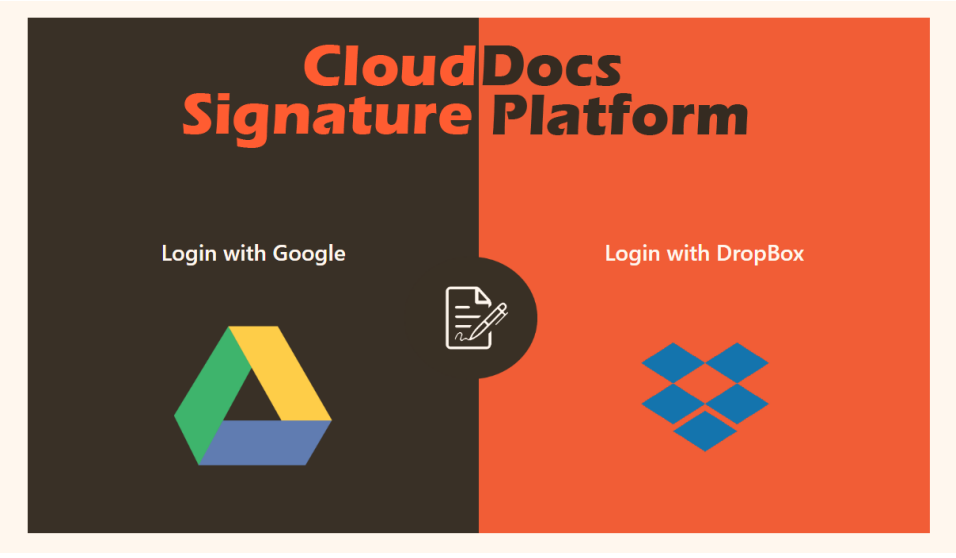
*FrontEnd:* està desenvolupat amb Laravel 5.7, un frameworks de PHP basat en Symphony. Permet fer login als diferents RS com Google, DropBox o TrustedX. Al ser la part visual de l'aplicació és l'encarregada de que l'usuari pugui realitzar totes les accions de manera fàcil i intuïtiva.

*BackEnd:* és una API RestFull, desenvolupada amb el framework d'SpringBoot, que segueix el patró de disseny Api Gateway. Aquest patró de disseny permet integrar diversos serveis semblants sota un mateix accés. D'aquesta manera l'API disposa del mateix mètode per obtenir fitxers independentment de si el repositori final de documents és Google Drive, DropBox o un altre RS. Per a la signatura de PDFs s'ha utilitzat la llibreria open source d'iText 7.1.4.

## Pantalles - Casos d'ús

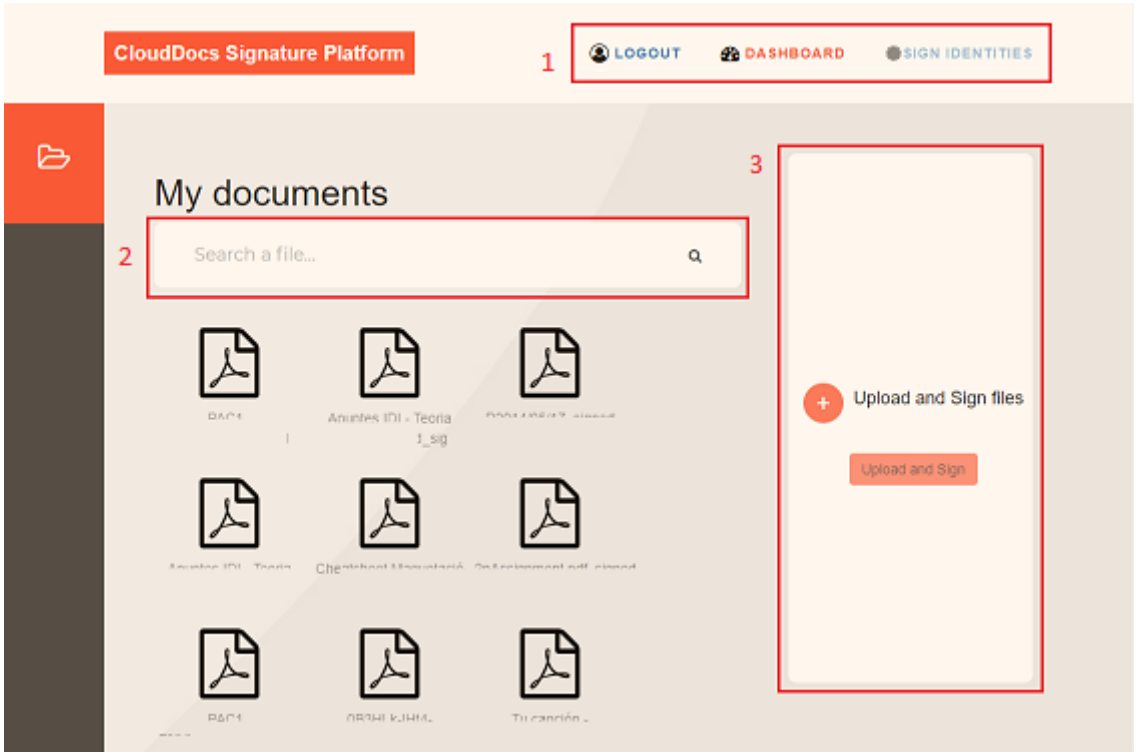
A continuació es detallen algunes captures de la interfície d'usuari desenvolupada per a permetre l'usuari la realització dels casos d'ús proposats

*Login*



L'usuari quan ha d'ingressar a l'aplicació realitza en un login en un dels serveis integrats en aquesta demo: Google Drive o DropBox. El login es realitza mitjançant Single Sign-On.

*Dashboard*



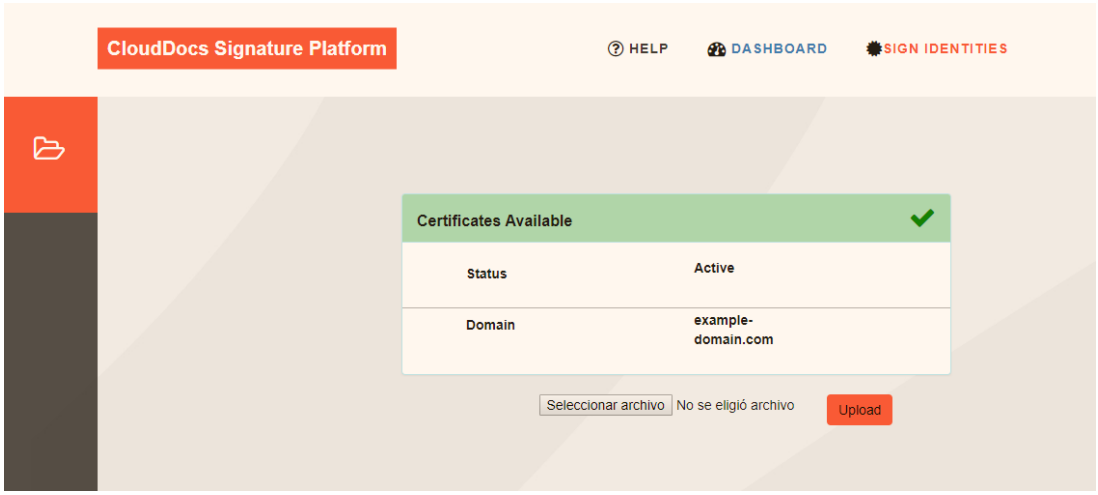

Un cop l'usuari ha fet login de manera exitosa a l'aplicació l'usuari accedeix al panell principal on pot veure els seus documents PDF. En aquesta pantalla, a més a més dels documents llistats inicialment trobem tres elements que permeten a l'usuari completar els casos d'ús:

1. Aquest panell permet a l'usuari fer Logout i moure's entre el Dashboard i el panell d'identitats en el qual carregarà les seves identitats de signatura de TrustedX.
2. Permet la cerca de documents en base al nom d'aquest. Ja pot ser usat per filtrar els documents llistats inicialment o per cercar-ne un que no aparegui a la llista.
3. L'usuari podrà pujar documents directament del seu dispositiu per a ser signats i incorporats a la servei de fitxers al qual s'ha accedit. En cas de no haver fet login amb l'aplicació TrustedX aquest panell esdevé inactiu.

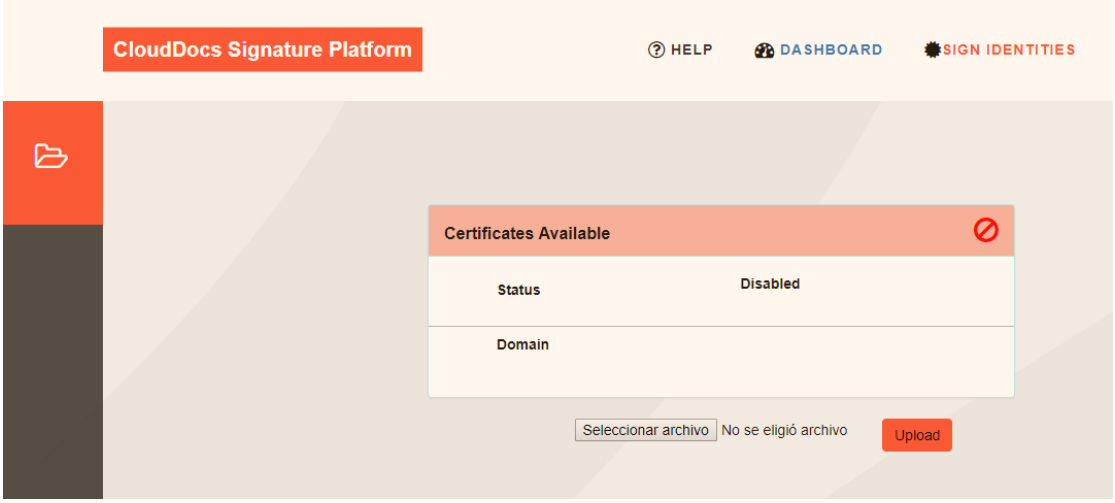
*Previsualització de PDFs prèvia a la signatura*


L'usuari pot seleccionar un document del panell per la seva previsualització, i en cas de voler, iniciar el procés de signatura. En cas de no haver fet login amb TrustedX l'acció de signar queda inactiva.

*Gestió d'identitats de signatura*



En aquest cas l'usuari disposa d'una identitat de signatura disponible a TrustedX i per aquest motiu el check surt en verd. En cas de no disposar de certificat l'usuari veuria com l'estat de la identitat és erroni. En aquest cas l'usuari hauria de pujar un certificat (en format pkcs12) seleccionant-lo del seu dispositiu i carregar-lo a TrustedX.

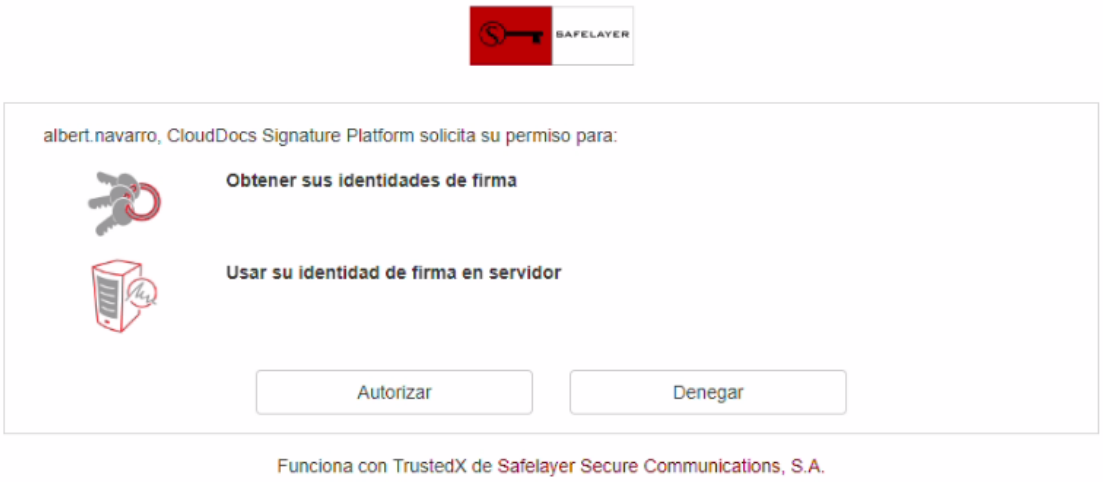



*Autorització d'accions amb TrustedX*

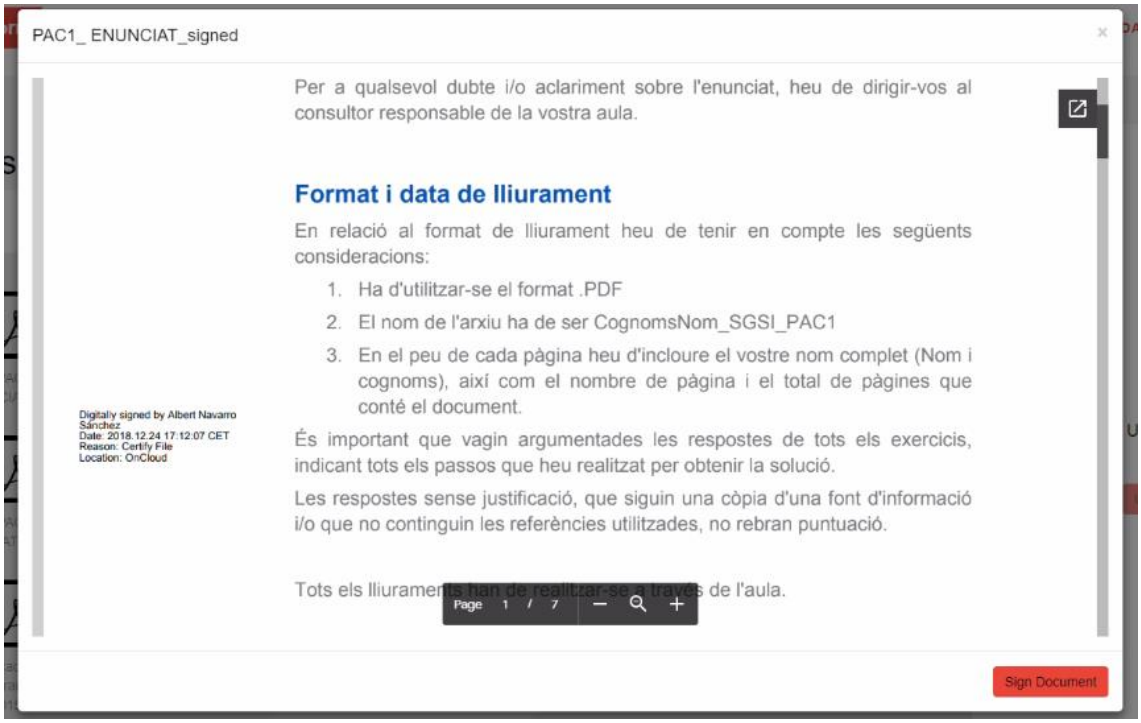
Totes les operacions que requereixen a l'aplicació consultar dades relacionades amb TrustedX, ja sigui per accedir a les identitats de signatura o per signar documents, necessiten d'una autorització expressa de l'usuari per a realitzar-se correctament.

Per exemple quan l'usuari accedeix al panell d'identitats de signatura haurà d'autoritzar l'operació :

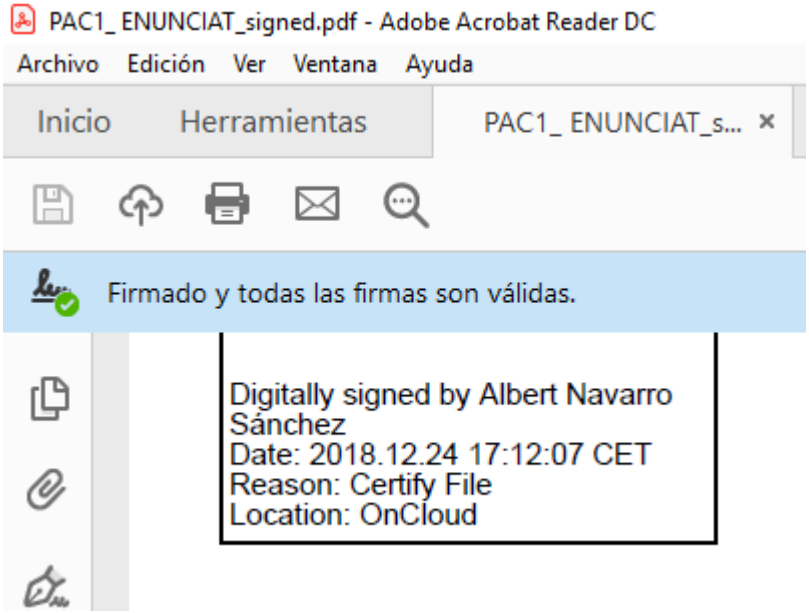
En aquest cas l'aplicació només requereix autorització per aquelles accions relacionades amb la gestió de les identitats de signatura i no demana autorització per a la signatura de documents. En canvi, quan l'usuari vol signar un document, els permisos s'adapten a les necessitats de l'acció que es vol realitzar:




*Visualització signatura*



Un cop signat el document es pot visualitzar des del mateix dashboard. Per una validació externa de la signatura s'ha utilitzat Adobe Reader havent afegit prèviament el certificat al llistat de confiança.



# Conclusions i treball futur

A l'inici del projecte s'exposava com els vectors Social, Mobile and Cloud podien ajudar a desplegar i accelerar l'èxit de la nova proposta del reglament eIDAS. En base a una arquitectura que engloba tots els elements necessaris per a la seva implementació CloudDocs Signature Platform és un prototip que prova la premises inicials del projecte. En aquest sentit, interconnectant diversos serveis de recursos, proveïdors d'identitat i serveis d'autorització i autenticació s'ha desenvolupat una solució que salva les dificultats principals de la signatura electrònica "tradicional" i aplica el reglament eIDAS per a la realització de signatures electròniques al cloud i sense la necessitat d'utilitzar dispositius externs.

El desenvolupament de l'aplicació ha avançat a bon ritme tot i haver trobat algunes dificultats en la generació de les signatures. El patró escollit pel desenvolupament del backend ha resultat encertat. Per tal de provar aquest patró primerament s'han desenvolupat totes les funcionalitats integrades només amb GoogleDrive, llavors s'ha afegit la integració amb Dropbox. L'esforç dedicat a aquest afegit ha estat el d'entendre l'API, més que el de dissenyar o remodelar el codi ja fet per incloure el nou driver.

Les funcionalitats desenvolupades en aquesta demo permeten una evolució de l'aplicació ja sigui afegint nous Resource servers o afegint funcionalitats que ofereixen les APIs com per exemple descarregar arxius o crear uns llistats de fitxers més interactius al panell principal.

El repte principal del projecte era aplicar el reglament eIDAS per poder signar documents directament al núvol sense haver de disposar ni dels documents dins el dispositiu ni de cap perifèric per a la signatura digital. El prototip resultant d'aquest projecte permet realitzar signatures electròniques avançades segons la definició donada pel reglament. No obstant, al ser un prototip no és capaç d'emetre signatures qualificades, per això un dels treballs futurs seria la implementació d'un LoA adient per arribar a l'escenari ideal, on l'aplicació seria viable i compliria els requisits de la llei al 100%.

Amb perspectiva, el projecte ha assolit l'objectiu principal d'obtenir una aplicació base que permetés estudiar com utilitzar els protocols d'autenticació com OAuth2, els servidors de recursos i un gestor d'identitats com TrustedX per tal d'ajustar-lo a la nova reglamentació eIDAS. L'opció de millorar i dotar d'un LoA superior a l'aplicació i l'evolució de les funcionalitats integrades dins l'aplicació deixa la porta oberta a estudiar les possibilitats d'aquest projecte més enllà d'una prova de concepte.

# Bibliografia

Anicas, Mitchell. “Una Introducción a OAuth 2.” N.p., 2018. Web.

Community, OAuth. “OAuth 2.0.” N.p., n.d. Web.

Dropbox. “DropBox API.” N.p., n.d. Web.

Google. “GoogleDrive API.” N.p., n.d. Web.

iText. “IText.” N.p., n.d. Web.

Jordan, Francisco, Helena Pujol, and David Ruana. “Identity Services: Electronic IDentification, Authentication and Signature (EIDAS) Achieving the EIDAS Vision through the Mobile, Social and Cloud Triad1.” *Safelayer Secure Communications S.A.* (2014): n. pag. Print.

Laravel. “Laravel 5.7.” N.p., n.d. Web.

“REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de Julio de 2014.” 2014: n. pag. Print.

Safelayer Secure Communications, S.A. “TrustedX EIDAS 4.1.4.1.” N.p., n.d. Web.