SignaDoc

App per a Signatura Digital de Documents en Android

Santiago Jurado Defez
Màster Universitari en Enginyeria Informàtica
TFM-Desenvolupament d'Aplicacions sobre Dispositius Mòbils

Consultors
Jordi Ceballos Villach
Jordi Almirall López

Professor
Robert Clarisó Viladrosa

Data Lliurament
15-06-2016

FITXA DEL TREBALL FINAL

Títol del treball:	*SIGNADOC*
Nom de l'autor:	*Santiago Jurado Defez*
Nom dels consultors:	*Jordi Ceballos Villach* *Jordi Almirall López*
Data de lliurament (mm/aaaa):	*06/2016*
Àrea del Treball Final:	*Desenvolupament d'Aplicacions sobre Dispositius Mòbils*
Titulació:	*Màster Enginyeria Informàtica*

Resum del Treball (màxim 250 paraules):

L'objectiu principal de aquest projecte és desenvolupar una aplicació Android que permeti a l'usuari signar digitalment documents PDF des de dispositius mòbils, d'una manera segura.

Com podem garantir l'autoria i identitat de la persona que signa el document, la integritat del mateix i al mateix temps mantenir la facilitat d'ús amb seguretat?

1. Utilitzant certificats digitals.
2. Autoritzant el seu ús mitjançant la nostra empremta dactilar.
3. Fent un disseny centrat en l'usuari.

Abstract (in English, 250 words or less):

The main goal of this project is to develop an application Android that allow to the user sign digitally documents PDF since mobile devices, of a safe way.

How we can guarantee the autor and identity of the person that signs the document, the integrity of the same and be able to keep the ease of use with security?

1. Using digital certificates.
2. Authorising his use by means of our finger print.
3. Doing a design centred in the user.

Paraules clau (entre 4 i 8):

FingerPrint, KeyStore, Android, PDF, private and public key, sign, digital certificates.

Índex

Llista de figures

1. Introducció

1.1 Context i justificació del Treball

Encara que l'ús de certificats digitals està cada vegada més estès en l'àmbit professional, encara existeix una bretxa digital que frena l'adopció d'aquesta tecnologia. Generalment utilitzem els certificats digitals per realitzar tràmits amb les administracions públiques i existeixen serveis públics en línia que de vegades són difícils d'accedir i usar, per la qual cosa l'experiència d'usuari no és la millor.

L'ús de certificats digitals ens permet signar documentació sense estar present físicament i al mateix temps assegurem l'autoria i identitat de la persona que signa el document i la integritat del mateix.
Si ha aquests avantatges li afegim l'opció de realitzar la signatura des del nostre smartphone o tauleta, d'una manera segura, aconseguim agilitar i processar signatures de múltiples documents de forma més ràpida.

L'objectiu final d'aquesta aplicació és dotar a l'usuari d'una plataforma per a la signatura digital de documents que sigui amigable, segura, transparent i que generi la suficient confiança perquè l'adopti.

Alternatives al mercat:

L'aplicació la funcionalitat de la qual més s'assembla a la d'aquest projecte és la app Signatura Digital FMNT, creada per l'espanyol Alfredo Muñoz Andrades. El llistat de funcionalitats és pràcticament el mateix que el d'aquest projecte, però és una aplicació de pagament, encara que barata, i que té copyright, per la qual cosa no és possible utilitzar-la de punt de partida per afegir-li funcionalitats. Està totalment orientada a utilitzar certificats emesos per la FNMT de Espanya.

Figura 1: App Firma Digital FNMT

1.2 Objectius del Treball

L'objectiu principal de aquest projecte és desenvolupar una aplicació Android que permeti a l'usuari signar digitalment documents des de dispositius mòbils, com per exemple, conformar factures, comandes, pressuposats etc.

A nivell personal, m'agradaria adquirir cert nivell de coneixements del desenvolupament d'aplicacions en Android, així com en criptografia i identitats digitals. Amb més precisió, estudiaré les Android Cryptography API, Android FingerPrint API i aquelles llibreries de codi obert, que em permetin manipular documents PDF.

Finalment, m'agradaria deixar a la disposició de la comunitat una aplicació de codi obert, que pugui servir de base a futurs desenvolupaments en els quals la signatura digital es pugui integrar com una utilitat més del sistema, com pot ser la geolocalització i pugui ser utilitzada des d'altres aplicacions, com el correu electrònic, per eixample.

Funcionalitats

Per a la primera versió de la App, anem a utilitzar el format de signatura PAdES (advanced electronic signatures for PDF documents). El motiu principal, és que els fitxers pdf són molt coneguts, qualsevol document generat per les principals suites ofimàtiques pot ser fàcilment convertit a aquest format, es pot generar un resum visual de la signatura en el propi document i a més el destinatari pot comprovar fàcilment la signatura i el document signat.

El tipus de certificat que es va a utilitzar és el certificat d'usuari X.509.V3.
Aquest tipus de certificat és el que expedeix de manera gratuïta la FNMT a tots els ciutadans que ho sol·licitin (Certificat FNMT Classe 2 CA) i la pròpia administració proveeix la possibilitat de descarregar-ho directament en dispositius Android, mitjançant una App anomenada "Obtención Certificado FNMT para Android", que ens podem descarregar des de Google Play. (1)

Figura 2: Obtenció certificat FNMT

El procés principal per a l'usuari consistirà en els següents passos:

Figura 3: Procés principal signatura

Per al procés de signatura, el sistema sol·licitarà que l'usuari utilitzi la seva empremta dactilar per signar el document. En el cas que la empremta obtinguda es correspongui amb l'emmagatzemada en el dispositiu es procedirà a la signatura del document. D'aquesta manera, es

facilita l'ús segur dels mateixos, eliminant la necessitat d'introduir el nombre PIN associat al certificat digital mitjançant el teclat del mòbil, la qual cosa comporta que molts usuaris utilitzin contrasenyes febles, del tipus 1234, 1111, per fer ús del certificat i millora l'experiència d'usuari.

El document signat tindrà una marca visible amb el resum de la signatura i finalment el document es guardarà amb el mateix nom de document original afegint "_signat.pdf".

Les funcionalitats secundaries de la aplicació seran les següents:

- Manteniment de certificats instal·lats
- Registre i assegurança de les claus dels certificats
- Selecció de certificat per a signatura
- Definició de certificat per defecte
- Selecció/Exploració de fitxers
- Signatura de Documents
- Encriptació de Documents

Encara que se surt de l'àmbit d'aquest projecte, seria interessant ampliar la funcionalitat de l'aplicació, acceptant els formats de signatura XAdES, OOXML i ODF.

> *XAdES (XML Avançat)*
> *El resultat és un fitxer de text XML, un format de text molt similar a l'HTML que utilitza etiquetes. Els documents obtinguts solen ser més grans que en el cas de CAdES, per això no és adequat quan el fitxer original és molt gran. Aplicacions com eCoFirma del Ministeri d'Indústria i Comerç, només signen en XAdES.*
>
> *OOXML i ODF*
> *Són els formats de signatura que utilitzen Microsoft Office i Open Office, respectivament.* (2)

Plataforma de desenvolupament

Per a la realització d'aquest projecte vaig a utilitzar el IDE Antroid Studio versió 2.1.2, que és la ultima versió estable publicada, instal·lada sobre un sistema operatiu Windows 8.1 i en un PC HP Probook 4540s amb 8 GB de RAM.
La plataforma destino és Android 6, ja que és la primera a oferir la Fingerprint Authentication en la seva API. A dia d'avui és l'última versió del sistema operatiu.

Figura 4: Android Studio

1.3 Enfocament i mètode seguit

Les principals aproximacions per a la signatura de documents mitjançant certificats digitals, en entorns mòbils són dos:

1. El desenvolupament d'una aplicació nativa/híbrida que tingui accés als certificats digitals emmagatzemats en el dispositiu i les seves claus privades.
2. El desenvolupament d'un sistema de signatura en el núvol, en el qual l'usuari puja a un servidor segur els seus certificats, claus privades i tots els documents que vol signar, per la qual cosa únicament necessita una connexió al servei mitjançant un navegador web.
   Aquesta aproximació s'utilitza principalment per empreses privades, sent els clients els seus propis empleats i elles mateixes les entitats certificadores, com per eixample la plataforma per a la signatura de contractes utilitzada per l'empresa de treball temporal Randstat. (3)
   Encara que el passat 18 de juliol es va modificar la llei 25/2015, per donar cobertura legal a l'emmagatzematge per part de tercers de certificats i claus privades emeses per administracions públiques o privades:
   El objetivo de esta modificación es dar un soporte jurídico sólido a la llamada "firma en la nube", en la que la clave privada del firmante no residirá físicamente en su equipo, si no en un servidor de confianza. (4).

L'estratègia triada per cobrir els objectius principals del projecte consisteix a desenvolupar una nova aplicació Android. Amb això aconseguiré aprofundir en els meus coneixements de signatura i xifrat digital, que puc aprofitar en altres projectes en la meva carrera professional i consolidaré els meus coneixements en disseny d'interfícies i usabilitat, en dissenyar en un entorn, com és el desenvolupament d'aplicacions mòbils, molt orientat a obtenir una experiència d'usuari òptima.

1.4 Planificació del Treball

La planificació temporal del projecte ve marcada per les dates de lliurament de les diferents PAC, que es converteixen en fites del projecte, i que ja han estat calculades pels tutors del projecte perquè s'ajustin al cicle de vida del desenvolupament de la aplicació i la documentació associada.
Com el marc temporal ve definit, i és inflexible, la dificultat consisteix a controlar l'àmbit del projecte perquè el contingut sigui el suficient per obtenir un producte que compleixi les expectatives dels consultors i no sigui tan ambiciós que ens aboqui al fracàs per falta de recursos.

Tenint en compte que el projecte és individual, les circumstàncies personals de l'alumne marcaran el temps que pot comprometre. En el meu cas particular, tenint en compte la meva situació laboral i familiar, puc dedicar els següents recursos setmanals:

- Dilluns: 2 hores
- Dimarts: 1 hores
- Dimecres: 2 hores
- Dijous: 1 hores
- Divendres: 3 hores
- Dissabte: 7 hores
- Diumenge: 4 hores

el que implica un total de 20 hores setmanals, i unes 300 hores de dedicació des del lliurament del pla de treball fins el lliurament final.
Com sempre hi ha imprevists, em reservo dies de vacances per poder utilitzar-los durant el desenvolupament del projecte.

Les dates clau del projecte segons el Pla docent son les següents:

Dates clau

Activitats avaluables

Títol	Inici / Enunciat	Lliurament	Solució	Qualificació
PAC1: Pla de Treball	24/02/2016	09/03/2016	-	16/03/2016
PAC2: Disseny i arquitectura	09/03/2016	06/04/2016	-	13/04/2016
PAC3: Implementació	06/04/2016	18/05/2016	-	25/05/2016
Lliurament Final	18/05/2016	15/06/2016	-	-

Activitats no avaluables

Títol	Inici / Enunciat	Lliurament	Solució
Defensa Virtual	27/06/2016	01/07/2016	-

Figura 5: Dates clau projecte

I aquesta planificació ens marca tot el cicle de desenvolupament del projecte.
La planificació detallada es la següent:

Nombre de tarea	Duración	Comienzo	Fin
PFM	**322 horas**	**mié 24/02/16**	**mié 15/06/16**
PAC1: Pla de Treball	**42 horas**	**mié 24/02/16**	**mié 09/03/16**
Document amb la proposta del projecte	17 horas	mié 24/02/16	dom 28/02/16
Redacció Pla de Treball	20 horas	lun 29/02/16	dom 06/03/16
Instalació entorn de treball	2 horas	lun 07/03/16	lun 07/03/16
Desenvolupament app dummy	1 hora	mar 08/03/16	mar 08/03/16
Revisió i lliurament de la PAC	2 horas	mié 09/03/16	mié 09/03/16
PAC2: Disseny i arquitectura	**80 horas**	**jue 10/03/16**	**mié 06/04/16**
Analisi funcional	34 horas	jue 10/03/16	dom 20/03/16
Disseny de fluxe de treball	20 horas	lun 21/03/16	dom 27/03/16
Disseny gràfic	20 horas	lun 28/03/16	dom 03/04/16
Redacció i lliurament de la PAC	5 horas	lun 04/04/16	mié 06/04/16
PAC3: Implementació	**120 horas**	**jue 07/04/16**	**mié 18/05/16**
Implementació de la aplicació	75 horas	jue 07/04/16	dom 01/05/16
Testing	40 horas	lun 02/05/16	dom 15/05/16
Redacció i lliurament de la PAC	5 horas	lun 16/05/16	mié 18/05/16
Lliurament Final	**80 horas**	**jue 19/05/16**	**mié 15/06/16**
Revisió i millora de la aplicació	20 horas	jue 19/05/16	mié 25/05/16
Redacció manual d'usuari	4 horas	jue 26/05/16	vie 27/05/16
Redacció definitiva de la memoria	26 horas	sáb 28/05/16	sáb 04/06/16
Presentació	**24 horas**	**dom 05/06/16**	**dom 12/06/16**
Video aplicació	13 horas	dom 05/06/16	vie 10/06/16
Diapositives	11 horas	sáb 11/06/16	dom 12/06/16
Redacció i llirament de la PAC	5 horas	lun 13/06/16	mié 15/06/16
Defensa Virtual	18 horas	lun 27/06/16	vie 01/07/16

Figura 6: Planificació temporal

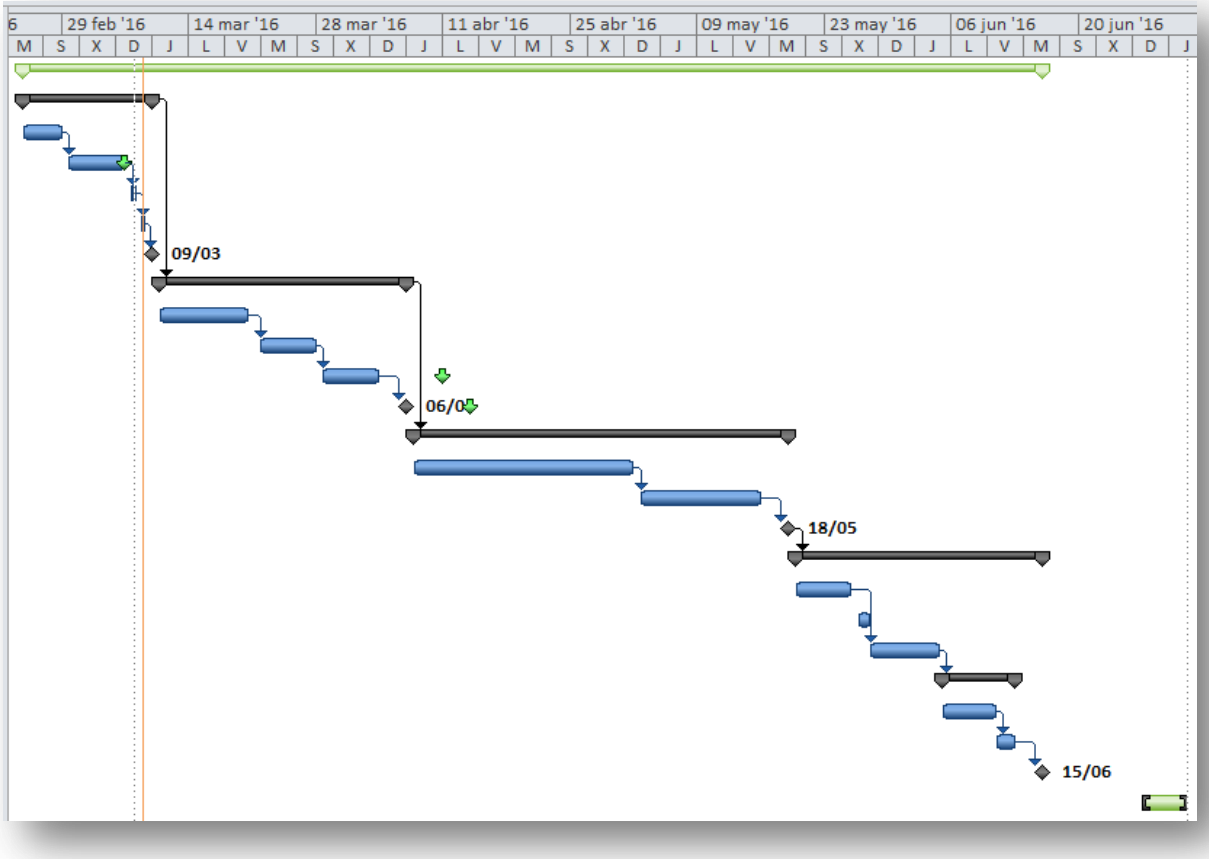


Figura 7: Diagrama de Gantt

1.5 Breu sumari de productes obtinguts.

A la finalització del Projecte Final de Master, està prevista el lliurament dels següents productes:

1. Aplicació Android per a signatura de documents.
2. Documentació de l'aplicació
    a. Manual d'usuari.
    b. Vídeo d'ús
    c. Presentació resumida en diapositives.
3. Memòria del projecte.

1.6 Breu descripció dels altres capítols de la memòria

Aquest document es distribueix en 5 capítols segons com s'exposa a continuació:

Capítol 1: Introducció.
En aquest capítol es realitza una introducció que explica a molt grans trets les característiques d'aquest projecte: quin és la motivació per al desenvolupament d'una aplicació per a l'ús d'identitats digitals, els objectius que es persegueixen, la metodologia duta a terme, que contribució aporta aquest projecte i com és la planificació temporal del mateix.

Capítol 2: Anàlisi

En aquest capítol estudiaré les llibreries Android de criptografia, que permeten realitzar funcions i aplicacions relacionades amb l'encriptació i signatura digital, els diferents mètodes de signatura digital, en què consisteix una identitat digital, l'ús segur de la identitat digital, etc., és a dir, s'estudia el context en el qual es va a desenvolupar l'aplicació. També s'explica que eines permeten l'ús i gestió de certificats digitals i com obtenir una identitat digital.
Es farà un disseny centrat amb l'usuari que es un enfocament de disseny, el procés del qual està dirigit per informació sobre les persones que van a fer ús del producte.
També es realitzarà una primera fase de prototipat de la interfície d'usuari, flux de navegació per les diferents pantalles, i un anàlisi detallat de les funcionalitats de l'aplicació.

Capítol 3: Disseny.

En aquest capítol es fan els casos d'ús de l'aplicació i descrivim l'arquitectura que tindrà i quines relacions tindrà amb la resta del sistema operatiu.

Capítol 4: Implementació.

En aquest capítol s'explica el disseny i desenvolupament de l'aplicació per a l'ús d'identitats digitals en la signatura de documents.

Capítol 5: Proves

En aquest capítol es mostren les proves a les que s'ha somes l'aplicació i quin es el resultat obtingut.

Capítol 6: Conclusions

En aquest capítol s'expressen les conclusions a les quals es ha arribat després de la realització del projecte i les possibles millores que es poden realitzar en el futur.

2. Anàlisi

2.1 Metodologia de desenvolupament

L'enfocament emprat per al desenvolupament del projecte és el disseny centrat en l'usuari DCU.

El Disseny Centrat en l'Usuari (DCU), o User Centered Design (UCD), és definit per la Usability Professionals Association (UPA) com un enfocament de disseny el procés del qual està dirigit per informació sobre les persones que van a fer ús del producte.

El concepte DCU tracta d'una filosofia de disseny que no té una especificació clara a l'hora de portar-la a la pràctica. Es parla del DCU com una filosofia perquè partim d'una premissa que condicionarà totes les nostres accions: l'usuari ha de situar-se al centre de tota decisió de disseny. No només dissenyem productes, dissenyem experiències d'usuari, perquè no és possible entendre el producte desvinculat del seu ús, el seu context, o de les necessitats i motivacions de l'usuari final. D'aquesta manera, l'enfocament del DCU persegueix assegurar la consecució d'un producte amb la funcionalitat adequada per a usuaris concrets.

Malgrat denominar-se "disseny", en realitat s'aplica durant totes les fases del desenvolupament (planificació, disseny, desenvolupament, avaluació), des de les primeres etapes, i té les següents característiques:

- És iteratiu.
- És multidisciplinari.
- El seu objectiu és obtenir productes usables i satisfactoris per als usuaris.

Amb aquestes característiques, les metodologies de desenvolupament que millor s'adapten a aquest enfocament són les anomenades àgils. (5)

2.2 Usuaris i context d'ús

2.2.1 Mètodes d'indagació

Observació i investigació contextual

Un dels mètodes que he triat ha segut el d'**observació i investigació contextual**, ja que tinc la possibilitat de fer l'estudi al meu lloc de treball. Aquest tipus d'usuari, utilitzarà la aplicació de signatura digital com a part de les seues tasques professionals, per la qual cosa, no he vist necessari ampliar l'estudi als seus hàbits fora de l'horari laboral.

Plantejament: L'exemple més proper, és la meva pròpia empresa, on actualment hi ha un procediment d'autorització de comandes que consisteix en una cadena de signatures manuals i autoritzacions molt lent. Aquest procés em servirà de base per a l'estudi, ja que l'objectiu final de la aplicació es substituir la signatura manual per la digital

Desenvolupament: He parlat amb tots els actors del procés de signatura i aprovació d'una comanda a un proveïdor. És un procés totalment manual:

1. Es generen els documents per mitjans telemàtics: word, excel, ...
2. S'imprimeixen els documents en paper
3. Se signen manualment per tots els actors, segons procediment.
4. Quan s'han completat les signatures, el document s'escaneja i s'envia al proveïdor per correu electrònic.

Perfil dels usuaris que fan ús d'aquest procediment:

1. Empleats tècnics e enginyers: Son els que comencen el procés. Tots tenen titulació universitària, treballen als departaments tècnics de l'empresa, logística, qualitat e

enginyeria. La distribució per sexes es prou paritària, tenen un alt perfil tècnic i fan un ús molt avançat de les noves tecnologies. Tots tenen PC portàtil i smartphone d'empresa.

2. Membres del equip de direcció: Son els que més documents signen, ja que normalment son responsables de departaments i tenen que autoritzar les comandes i pagament de factures. El perfil es similar al del grup anterior, amb l'única diferencia de que els smartphones i ordinadors son de gama més alta que per la resta d'empleats. També se està introduint la tauleta com a dispositiu d'ús habitual en el seu dia a dia.

Resultats:

- Tots els actors coincideixen que la implantació de la signatura digital suposaria un augment de la productivitat.
- La possibilitat de realitzar aquesta signatura des de mitjans mòbils és molt apreciada per aquells empleats que tenen llocs de responsabilitat en l'empresa i pels que tenen molta mobilitat.
- L'ús de la signatura digital per si a soles, no seria suficient, ja que es necessitaria la implantació d'algun tipus de programari de gestió documental, que ajudi a automatitzar els fluxos d'aprovació.

Conclusions:

Si representéssim gràficament la tasca de signatures de documents en una empresa, obtindríem una piràmide invertida, on uns pocs generen documentació que ha de seguir un flux d'aprovació, situant-se en llocs jeràrquics intermedis, i aquells empleats situats en la part alta de la jerarquia tenen grans quantitats de documents per signar. Aquest últim tipus d'empleat és el que té horaris més flexibles, el que realitza més tasques fora de la seva oficina i al que se li dota de millors recursos tecnològics (millor ordinador, millor smartphone, tablets, etc) i sol ser un coll d'ampolla en els fluxos d'aprovació. Tenen la capacitat d'impulsar aquells canvis en l'organització que tenen el seu interès.

Els usuaris utilitzen tots els mitjos digitals dels que disposen, encara que fan un ús d'un dispositiu diferent segons la tasca que fan i el lloc on es troben. Per eixample, se usa molt el mòbil per a llegir el correu i mantenir conversacions amb la resta d'usuaris del departament (utilitzem la variant professional del skype). La signatura digital de documents es una tasca candidata per a ser utilitzada en el mòbil o tauleta, ja que es una tasca molt lligada a la lectura del correu, on vindran els avisos per a signar documents, dins dels procediments empresarials.

Dinàmica de grup

També estic interessat en l'ús de la aplicació fora del àmbit empresarial, i he trobat grups d'interès amb aquesta tecnologia, com per eixample el AMPA del col·legi del meu fill, del que formi part. Aquest col·legi és d'àmbit supracomarcal, per la qual cosa els membres del mateix estan repartits per poblacions allunyades entre si, i la possibilitat de signar documentació d'una forma còmoda des del mòbil agilitzaria de manera notable les relacions amb el col·legi i l'administració. En aquest cas he triat el mètode de **Dinàmica de grup**, ja que com he dit jo també formi part d'aquest grup, la qual cosa em facilita molt la tasca.

Plantejament: He aprofitat l'última reunió de l'AMPA, per sondejar la possibilitat de signar digitalment la documentació que es remet l'adreça del col·legi, i que ha de ser prèviament analitzada i debatuda per l'adreça de l'AMPA. A causa de la naturalesa del col·legi, aquests debats els fem mitjançant WhatsApp i quan arribem a un acord sobre qualsevol proposta que ens fa arribar la direcció del centre, els membres de la directiva de l'AMPA, han de signar el document. Realitzar aquest procés amb el mòbil des de casa és vist com una gran millora pels membres d'aquest grup.

Desenvolupament: Hem realitzat una tempesta d'idees, perquè em donessin la seva visió de com podrien dur a terme la signatura de documents pel mòbil.

Cal tenir en compte que el perfil d'aquests usuaris és molt heterodox i que entenen perfectament l'ús i abast d'una signatura manuscrita, però el concepte d'identitat digital no ho tenen molt clar, per regla general.
Perfil dels usuaris que fan ús d'aquest procediment:

1. Usuaris amb baixa experiència digital: Normalment son persones amb una edat per damunt dels 40 anys. Encara que tots en el grup tenen mòbil, fan un ús bàsic del mateix. El gasten per a fer cridades i per xatejar al Whatsapp bàsicament. No fan ús intensiu del correu electrònic.
2. Usuaris amb un alt ús digital: Aquests usuaris son els més joves dins del grup, i tots tenen ordinador i tauletes a casa, i smartphones de gama mitjana/alta. Fan un ús intensiu de les xarxes socials i estan acostumats a treballar amb correu electrònic, programari de missatgeria i normalment son sempre connectats a internet.

Resultats:

- Des de el seu punt de vista, signar un document digitalment, ve a ser paregut a donar-li al "M'agrada" del Facebook. Es clar que estem parlant de documentació amb poques implicacions legals, però em crida l'atenció la simplificació del procés que fan.
- Com quasi tota la dinàmica del grup es fa per Whatsapp, el que han demanat es que sigui aquest el context d'utilització de la signatura digital. Es a dir, enviar els documents dins del grup de missatgeria i signar-los sense eixir-se de la aplicació.
- La part de configuració de la aplicació, com es la descarrega del certificat digital i el seu emmagatzematge en el dispositiu la veuen molt complicada.

Conclusions:
Aquest tipus d'usuari està començant a veure les possibilitats que les noves tecnologies tenen per facilitar les tasques diàries. Esperen que l'ús de les aplicacions sigui totalment amigable, amb una corba d'aprenentatge baix i que l'aplicació de signatura s'integri amb les aplicacions que usen habitualment en el seu telèfon.
Evidentment, l'integrar l'aplicació de signatura digital amb WhatsApp se surt de l'àmbit d'aquest projecte, però és clar que els usuaris cada vegada estan més acostumats al fet que les aplicacions comparteixin funcionalitats.
En fer l'estudi de grup, ha aparegut una nova problemàtica relacionada amb l'ús de l'aplicació: En el cas d'estudi anterior, les signatures seguien un ordre seqüencial i jeràrquic, per la qual cosa el document anava agregant les mateixes, però si envies un document a més d'un signant alhora, anem a obtenir diverses còpies del document amb diferents signatures, però cap amb totes.
L'única solució a aquest problema és que el secretari vagi sol·licitant les signatures seqüencialment als signants.

Anàlisi competitiva

Per a completar l'estudi he fet un **anàlisi competitiva**, però no més he considerat la part de valoració d'usuaris, ja que considero que m'ajudaran els comentaris dels usuaris d'aquestes aplicacions per a detectar les seues expectatives i a més em permetrà veure les tendències del mercat.
Plantejament: he revisat les app de signatura digital i la que té una funcionalitat més pareguda al propòsit d'aquest projecte es la "Firma digital FNMT", com ja vaig comentar en el capítol anterior.
Desenvolupament: He revisat les opinions dels usuaris de la app. En el moment d'escriure aquestes línies, n'hi ha 14 valoracions, amb una mitja de 4,4 punts sobre 5.

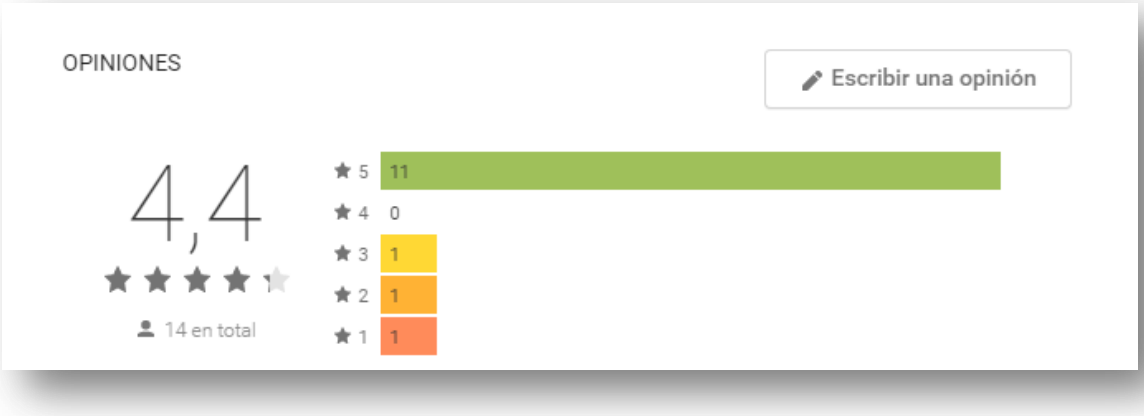


Figura 8: Opinions usuaris de l'App "Firma Digital FNMT"

Resultats: Les característiques mes apreciades pels usuaris son:

- Facilitat d'ús, alta productivitat i funcionalitat ajustada a les necessitats dels usuaris.
- Possibilitat de triar el lloc on s'imprimeix la signatura.
- Comoditat de signar documents des del mòbil o tauleta.

Alguns usuaris, demanen que es pugi afegir una imatge amb la signatura manual, encara que no té validesa legal

Conclusions:
Encara que el nombre de opinions no es molt significatiu i el nombre de instal·lacions es xicotet, pot ser per estar massa orientada a la instal·lacions de certificats de la FNMT, el que més valoren els usuaris es la facilitat d'ús i les avantatges que una aplicació amb una funcionalitat tan ajustada signifiquen per a la seua productivitat.
Les opinió més negativa es d'un usuari que diu que no li funciona per que la aplicació li diu que no té cap certificat instal·lat en el mòbil. N'hi haurà que cuidar el procés de selecció del certificat i emmagatzematge del seu PIN associat.

2.2.2 Fitxes de perfil d'usuari

PERFIL:	Usuari professional

CARACTERÍSTIQUES:

Usuaris que utilitzen mitjans digitals assíduament, formen part d'organitzacions amb un alt grau d'implantació tecnològica i automatització de processos.
Aquests usuaris solen tenir titulacions universitàries, estan acostumats a utilitzar procediments rigorosos de funcionament en el seu treball diari i solen utilitzar certificats digitals per comunicar dades amb les administracions públiques o amb grans clients.

CONTEXT D'ÚS:

Els usuaris faran ús d'aquesta aplicació per a signar documentació interna com pressupostos, comandes, factures, etc. Normalment rebran una sol·licitud de signa per correu electrònic amb el document adjuntat.
També se utilitzarà per a signar documents que tinguin com a destinatari l'administració pública. Son partidaris d'utilitzar el mòbil i fer-ho en hores mortes, com per exemple, mentre estan esperant un avió, abans de començar una reunió amb un client,... També farien ús de la aplicació fora de l'horari laboral, en vacances, etc.

ANÀLISI DE TASQUES:

- Registrar i emmagatzemar certificats digitals [T3]
- Recerca de fitxer per a signar [T1]
- Signatura de fitxers [T4]
- Encriptació de fitxers [T5]
- Emmagatzematge dels PIN [T3]
- Accés segur al procés de signatura [T3]

CARACTERÍSTIQUES DESCOBERTES:

- Utilitzen més d'un certificat digital
- Volen utilitzar un únic PIN per a signar en qualsevol certificat
- Tenen interès en la possibilitat de encriptar el document, sobretot pels que tenen informació confidencial, mentre el document, signat o no, romangui en el mòbil o tauleta.
- Estan preocupats per les mesures de seguretat en cas de robatori o perduda del mòbil.

PERFIL:	Usuari pertanyent a organitzacions sense relació laboral

CARACTERÍSTIQUES:

Existeixen usuaris que són representants en organitzacions, i encara que no tenen una relació laboral amb les mateixes, si que necessiten signar documents. Aquest tipus d'usuaris tenen perfils tant des del punt de vista tecnològic com a acadèmic molt heterodoxos. La implantació d'aquest tipus de utilitats, sempre que vagin acompanyades d'una petita formació, i sigui liderada per les organitzacions de les quals formen part, solen tindre èxit, ja que en tenir un component de voluntariat solen estar molt motivats.

CONTEXT D'ÚS:

Dins de la mecànica de grup virtual a Internet, els usuaris rebran una missatge del administrador del grup, demanant-los que signin el document que els adjunten per correu electrònic. Prèviament ja s'ha discutit i consensuat en el grup el contingut del document. Els usuaris aniran signant el document, sent l'administrador l'encarregat d'anar remetent-ho, a tots els implicats. Els usuaris utilitzaran l'aplicació en els seus mòbils, normalment fora de l'horari laboral.

ANÀLISI DE TASQUES:

- Registrar i emmagatzemar un certificat digital i el seu PIN [T3]
- Recerca de fitxer per a signar [T1]
- Signatura del fitxer [T4]
- Recerca del fitxer signat per retornar-ho al remitent [T1]
- Configuració de carpetes per defecte per a fitxers pendents i signats. [T2]

CARACTERÍSTIQUES DESCOBERTES:

- Declaració de la carpeta on el client de correu electrònic o el WhatsApp deixa els fitxers adjunts, per a que l'aplicació l'obri automàticament quan fen la recerca de fitxer per a signar.
- Poder activar una opció de configuració que permeti l'esborrat del fitxer una vegada signat, per evitar que es quedin ocupant memòria en el mòbil.
- Declaració de la carpeta on l'aplicació deixi el fitxer una vegada signat, amb l'objectiu que sigui fàcilment trobat per l'usuari..

PERFIL:	Usuari genèric
CARACTERÍSTIQUES: Són usuaris que normalment necessiten fer ús de la signatura digital amb algun tràmit amb les administracions públiques i poden fer ús d'aquesta eina, estalviant-se cues i esperes. Es dedueix pels comentaris que els usuaris son xicotets empresaris (autònoms) i particulars. Els perfils dels que fan comentaris son quasi tots d'homes (deduït pel nom) i n'hi ha un perfil que es una empresa. No tinc accés a l'edat dels usuaris ni la seua experiència amb la tecnologia.	
CONTEXT D'ÚS: No tenim informació del context d'us d'aquests usuaris.	
ANÀLISI DE TASQUES: • Registrar i emmagatzemar un certificat digital i el seu PIN [T3] • Signatura del fitxer [T4]	
CARACTERÍSTIQUES DESCOBERTES: • Volen triar el lloc en el document on imprimir la signatura • Tenir la possibilitat de afegir una imatge de la seua signatura manuscrita	

2.2.3 Anàlisi de tasques:

Encara que estem en una fase primerenca de procés de recerca ja hem detectat que tasques seran les més habituals. A continuació farem una aproximació de quins són els passos necessaris per dur-les a terme:

T1. Recerca de fitxers

L'aplicació disposarà d'un navegador de fitxers que s'utilitzarà para:

1. Seleccionar la carpeta de Documents Pendents
2. Seleccionar la carpeta de Documents Signats
3. Seleccionar els fitxers que contenen els certificats digitals
4. Seleccionar els fitxers que volem signar, encriptar, esborrar o moure
5. Crear o esborrar carpetes

T2. Configuració de carpetes per defecte per a fitxers pendents i signats:

1. Obrir l'aplicació o tornar a la pantalla d'inici
2. Seleccionar l'opció de configuració

3. Seleccionar l'opció de carpeta de Documentes Pendents o la de Documents Signats i prémer sobre la icona de l'explorador de fitxers [T1]
4. S'obri un explorador de fitxers i se selecciona o crea un directori. En aquest directori l'aplicació mostrarà els document que n´hi ha en la carpeta de Documents Pendents o deixarà la còpia signada dels documents en la carpeta de Documents Signats.

T3. Registrar i emmagatzemar certificats digitals

1. Obrir l'aplicació o tornar a la pantalla d'inici
2. Seleccionar l'opció de configuració
3. Prémer en la icona de Certificats.
4. Seleccionar l'opció d'Afegir Certificat.
5. S'obre un explorador de fitxers i naveguem pel dispositiu per seleccionar el certificat [T1]
6. Una vegada seleccionat el certificat, l'aplicació ens demanarà el PIN associat a aquest certificat.
7. L'aplicació registrarà i emmagatzemarà el certificat i a partir d'aquest moment estarà disponible.
8. Si no més tenim un certificat registrat a l'aplicació, aquest serà el certificat per defecte i l'aplicació té una opció que es pot activar, per a utilitzar-ho sense preguntar a l'usuari.

T4. Signatura de fitxer

1. Obrir l'aplicació o tornar a la pantalla d'inici
2. Seleccionar l'opció de configuració
3. Seleccionar l'opció Signar | Encriptar
4. L'aplicació obrirà un explorador de fitxers [T1]. Si en la pantalla de configuració s'ha parametritzat una carpeta de Documents Pendents, l'explorador mostrarà aquesta, encara que permetrà navegar per tot el sistema de fitxers.
5. L'usuari podrà seleccionar els documents que vol signar.
6. En el següent pas, l'aplicació mostrarà un llistat dels certificats disponibles, perquè l'usuari seleccioni un.
7. A continuació haurà de triar l' acció de Signar:
8. A continuació l'aplicació sol·licitarà a l'usuari que utilitzi la mesura de seguretat triada en la configuració, per garantir un ús segur del certificat (PIN o escanejo d'empremta digital).
9. Si les mesura de seguretat és acceptada per l'aplicació, una còpia del fitxer amb la signatura digital es guardarà a la carpeta de Documents Signats.

T5. Encriptació de fitxer

1. Obrir l'aplicació o tornar a la pantalla d'inici
2. Seleccionar l'opció de configuració
3. Seleccionar l'opció Signar | Encriptar
4. L'aplicació obrirà un explorador de fitxers [T1]. Si en la pantalla de configuració s'ha parametritzat una carpeta de Documents Pendents, l'explorador mostrarà aquesta, encara que permetrà navegar per tot el sistema de fitxers.
5. L'usuari podrà seleccionar els documents que vol encriptar.

6. En el següent pas, l'aplicació mostrarà un llistat dels certificats disponibles, perquè l'usuari seleccioni un.
7. A continuació haurà de triar l' acció de Encriptar
8. A continuació l'aplicació sol·licitarà a l'usuari que utilitzi la mesura de seguretat triada en la configuració, per garantir un ús segur del certificat (PIN o escanejo d'empremta digital).
9. Si les mesura de seguretat és acceptada per l'aplicació, una còpia del fitxer encriptat es guardarà a la carpeta de Documents Encriptats.

2.3 Disseny conceptual

2.3.1 Escenaris d'ús

A continuació es detallen una sèrie de possibles escenaris d'ús de l'aplicació a desenvolupar.

Escenari 1	
Perfil:	Usuari professional
Context:	L'usuari es el director de l'empresa, es troba a la seua oficina i necessita configurar l'aplicació, per a funcionar de modo segur.
Objectius:	Configurar l'aplicació perquè tingui un comportament àgil i segur
Tasques:	Configuració de carpetes per defecte per a fitxers pendents i signats. Configuració del tipus de seguretat. Comportament de l'aplicació amb el tractament dels fitxers. Registrar i emmagatzemar certificats digitals.
Necessitats d'informació:	El director de l'empresa té necessitat de signar molta documentació i a més, molts dels documents que te que signar tenen caràcter confidencial, per la qual cosa, deuen estar protegits en cas de perduda o robatori del telèfon o tauleta.
Funcionalitats:	Omplir la pantalla de configuració de l'aplicació. Emmagatzemar els certificats.
Desenvolupament de les tasques:	

El Joan es el director de l'empresa AUTOTRIM i té que signar un muntó de documents de tot tipus al llarg del dia. Amb la finalitat de ser més productiu, relega totes les tasques de signatura per a ferles al final de la vesprada, o si està de viatge quan es troba en el tren, al hotel,...
Normalment li agrada utilitzar la tauleta per a fer aquestes tasques, ja que es més còmoda que el mòbil per a llegir els documents, però li preocupa la seguretat, ja que encara que té contrasenyes per accedir li fa por que li furten la tauleta amb documents confidencials dins.
Per assegurar-se que l'aplicació és segura i es comporta com ell necessita en el tractament dels documents, crida a un tècnic IT de l'empresa perquè li ajudi a configurar-la adequadament.

El tècnic li instal·la l'aplicació i li va ajudant amb els passos de la configuració.
La primera tasca consisteix a seleccionar el tipus de seguretat que es va a utilitzar. Com el director té un mòbil i una tauleta d'última generació, una vegada oberta l'aplicació va a la pantalla de configuració, prem l'opció seguretat i selecciona l'opció **Empremta Dactilar** per a l'opció de **Autentificació**. A partir d'aquest moment, l'aplicació sol·licitarà a l'usuari que escanegi la seva empremta dactilar cada vegada que vulgui realitzar algun tipus d'acció sensible, com utilitzar o esborrar un certificat digital.

La segona tasca consisteix a configurar les opcions de tractament de fitxers. Tornant a la pantalla de configuració, entrarem en la pantalla de configuració de fitxers. Seleccionarem les carpetes de **Documents Pendents** i **Documents Signats**, amb l'explorador de fitxers. També marcarem les opcions a realitzar amb els documents, per exemple:

- Esborrar (o no) document original una vegada signat.
- Esborrar (o no) document original una vegada encriptat.
- Deixar document signat a la carpeta Documents Signats, o a la mateixa carpeta on estava l'original.
- Deixar document encriptat a la carpeta Documents Signats, o a la mateixa carpeta on estava l'original.
- Seleccionar extensió de fitxer signat. Per defecte nomFitxer_sign.pdf
- Seleccionar extensió de fitxer encriptat. Per defecte nomFitxer_ncrp.pdf

La tercera tasca consisteix a registrar i emmagatzemar els certificats digitals que utilitzarà el director. Aquest utilitza 3 certificats, el d'empleat emès per l'empresa, el de representant de l'empresa i el personal, emesos tots dos per la FNMT. Amb l'ajuda del tècnic el director descarrega els certificats digitals en la tableta, obre l'aplicació i selecciona l'opció **Afegir Certificat Digital**. L'aplicació obre un explorador de fitxers i va buscant i seleccionant els certificats un a un. L'aplicació sol·licita el nombre PIN del certificat i els registra i emmagatzema.

Una vegada realitzats aquests passos, l'aplicació està configurada per realitzar la seva funció de manera ràpida i segura.

Escenari 2	
Perfil:	Usuari professional
Context:	L'usuari es troba de viatge al tren
Objectius:	Llevar-se de damunt tasques burocràtiques
Tasques:	Signar un document
Necessitats d'informació:	Necessita accedir al document original, signar-lo amb el certificat apropiat i després accedir al document signat.
Funcionalitats:	Selecció de fitxers Selecció de certificat Signatura
Desenvolupament de les tasques:	

La Begoña es la cap del departament de logística de l'empresa AUTOTRIM. Hui té una reunió en Barcelona amb uns clients de l'empresa i ha agafat el tren per anar.
Com a part del seu equipatge de ma du un maletí amb un portàtil i el smartphone corporatiu. Com el viatge de Valencia a Barcelona dura més de 3 hores, està revisant el seu correu electrònic al mòbil.
Li arriba un correu d'un dels seus col·laboradors demanant-li que aprovi una comanda per al lloguer d'un nou magatzem, ja que el de la empresa està saturat i ha trobat un a bon preu propet.
Begoña revisa el pressupost associat i quan comprova que tot es correcte, descarrega el document de la comanda, en format pdf, al seu mòbil. Acte seguit, obri la app SignaDoc. L'aplicació li mostra una pantalla d'inici i tria l'opció **Signar**. L'aplicació obri l'explorador de fitxers mostrant el contingut de la carpeta **Documents Pendents**, on troba la comanda i la

selecciona. Després pressiona el botó de Signar i l'aplicació li mostra els certificats que te emmagatzemats, que son dos: el seu personal expedit per la FNMT i el de empleat de AUTOTRIM que li proporcionaren des de el departament de RR.HH. Tria el certificat d'empleat i l'aplicació li demana l'escanejo de la seua empremta dactilar. Posa el dit damunt de l'escàner i l'aplicació li mostra un missatge informant-la que el document ha segut signat i s'ha deixat a la carpeta **Documents signats**. A continuació, tanca l'aplicació SignaDoc, obri l'aplicació de correu, i contesta al correu del seu col·laborador adjuntant-li la comanda signada. El col·laborador rep la contestació i la comanda signada 10 minuts després i la remet al departament jurídic per a que signen un contracte de lloguer amb els propietaris del magatzem.

Escenari 3	
Perfil:	Usuari pertanyent a organitzacions sense relació laboral
Context:	El usuari està gaudint del seu temps lliure, en casa o en qualsevol altre lloc on pugui estar connectat a Internet i utilitzar el mòbil. El usuari es membre de la directiva del AMPA del col·legi del seu fill, que es de àmbit supracomarcal.
Objectius:	Signar documents
Tasques:	Selecció de fitxer Signatura
Necessitats d'informació:	El usuari necessita signar documents des de el mòbil per a evitar desplaçaments i agilitzar les tasques
Funcionalitats:	Signar documents
Desenvolupament de les tasques:	

L'Arnau es el secretari de l'AMPA del col·legi del seu fill i una vesprada revisa el WhatsApp i veu que en el grup de l'AMPA el president ha escrit un missatge informant a la resta que, des de la directiva del centre han sol·licitat que l'associació realitzi una aportació econòmica al centre per a la festa de finalització de curs.
Durant un parell d'hores la resta de membres de l'AMPA realitza un debat sobre quant diners aportar i finalment arriben a un acord. El secretari rep l'encàrrec d'enviar un document a la directiva del centre, amb l'acord.
Des de la seua tauleta, genera un document amb Google Docs i ho descarrega en format pdf.
Obre l'aplicació SignaDoc, selecciona l'opció de Signar, l'aplicació obre l'explorador de fitxers i selecciona el document que ha descarregat. Quan prem sobre el botó signar, l'aplicació li demana el codi PIN de l'únic certificat que té instal·lat, i una vegada ho introdueix, l'aplicació li mostra un missatge confirmant que el document ha estat correctament signat.
Torna al WhatsApp, i li escriu un missatge al president per avisar-li que el document ja està preparat i enviar-li-ho.

El Lluis, president de l'AMPA, no té molta idea de com funciona la signatura digital, però l'Arnau els ha instal·lat i configurat a tota la directiva l'aplicació SignaDoc en els telèfons. Quan obre l'aplicació, selecciona l'opció de signar i l'explorador de fitxers s'obre automàticament a la carpeta **/scard/WhatsApp/media**, i mostra únicament els documents amb extensió pdf que es reben per WhatsApp. Selecciona el fitxer, prem el botó signar, i com l'aplicació té un únic certificat registrat i l'opció de **Signar Sense Preguntar** activada, l'aplicació li sol·licita el PIN i una vegada introduït, de seguida rep un missatge avisant que el document ha segut signat. Torna al WhatsApp i respon amb el document signat a l'Arnau.

Quan l'Arnau rep el missatge del Lluis, obre el seu client de correu electrònic en la tauleta, i envia un correu a la directiva del centre, adjuntant el document degudament signat pel president i ell mateix.

Escenari 4	
Perfil:	Usuari genèric
Context:	El usuari és un comercial autònom i representa a diverses empreses de distribució de maquinaria d'obres públiques. La seva tasca diària consisteix a visitar ajuntaments i empreses de serveis públics per fer ofertes de maquinària de neteja vial, en lloguer o venda.
Objectius:	Enviar pressupostos i ofertes vinculants amb signatura digital a administracions i empreses públiques.
Tasques:	Selecció de fitxer Signatura digital
Necessitats d'informació:	El usuari necessita enviar ofertes amb validesa legal des de el mòbil o tauleta per a que siguin acceptades per les administracions.
Funcionalitats:	Signar documents
Desenvolupament de les tasques:	

El Pep utilitza habitualment l'aplicació SignaDoc. Té declarats els certificats que li acrediten com a representant de vendes de totes les empreses per les quals realitza labors comercials. A més els certificats emesos per aquestes empreses, solen tenir un període de validesa curt, ja que hi ha molta rotació de comercials, i l'aplicació impedeix l'ús de certificats caducats.

Un matí visita l'àrea d'urbanisme d'un ajuntament del cinturó de València, ja que l'encarregat de manteniment vial, li ha cridat perquè necessita llogar urgentment una màquina per a la neteja viària, ja que la que posseeix l'ajuntament està avariada.

Una vegada finalitzada l'entrevista amb l'encarregat, i tenint clares les seves necessitats, prepara tres ofertes de tres maquines, perquè l'encarregat pugui seleccionar la que millor s'ajusti al seu pressupost. És important fer arribar les ofertes en el menor termini possible, perquè sap que és urgent i a més hi ha altres comercials oferint productes similars.

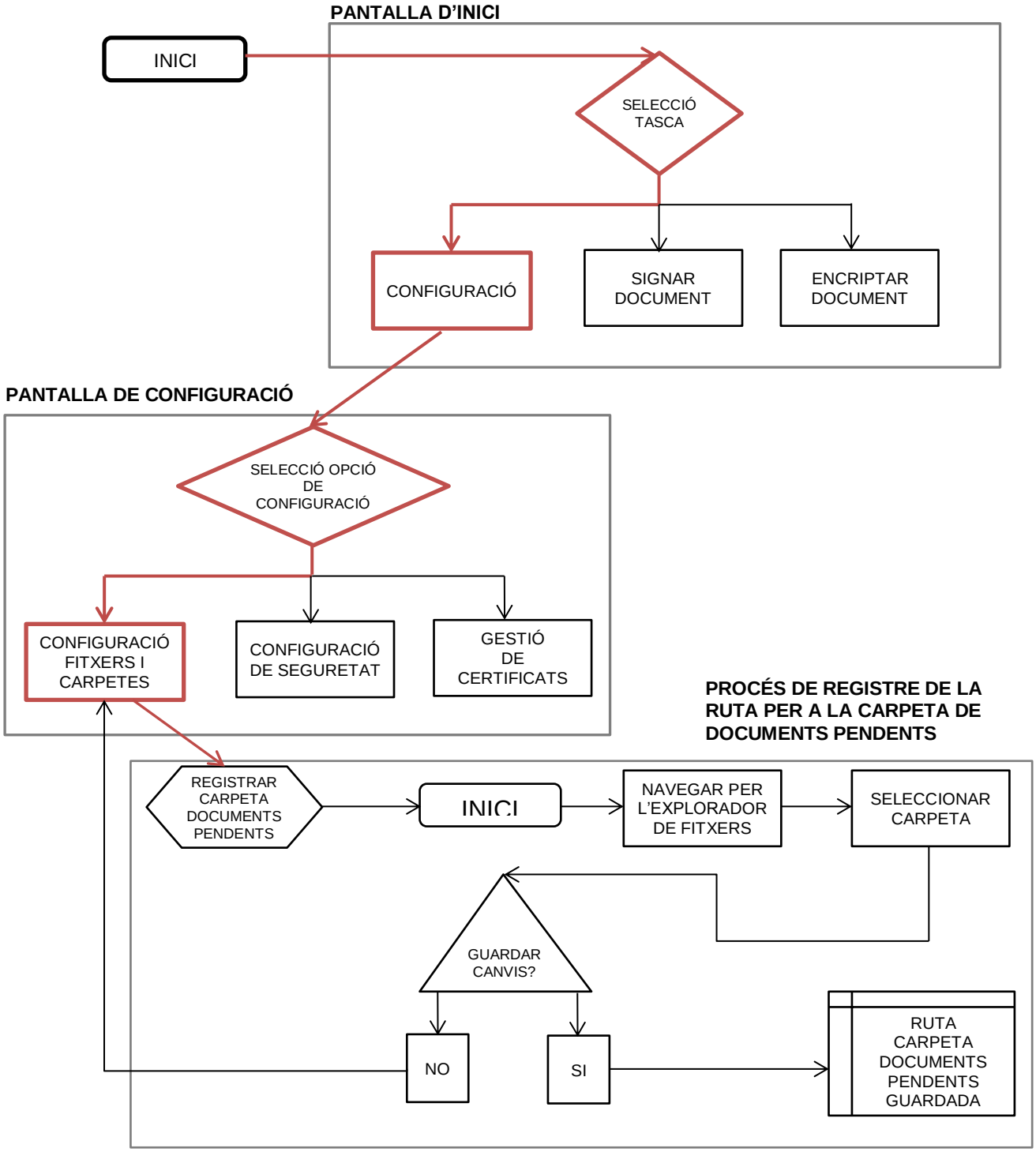
Des de la tauleta, obre l'aplicació que li mostra la pantalla d'inici i tria l'opció Signar. L'aplicació obri l'explorador de fitxers mostrant el contingut de la carpeta Documents Pendents, on troba les ofertes. Després pressiona el botó de Signar i l'aplicació li mostra els certificats que te emmagatzemats, i tria el certificat emès per l'empresa propietària de la màquina i l'aplicació li demana l'escanejo de la seua empremta dactilar. Posa el dit damunt de l'escàner i l'aplicació li mostra un missatge informant-la que el document ha segut signat i s'ha deixat a la carpeta Documents signats. Repeteix el procés amb la resta d'ofertes, A continuació, tanca l'aplicació SignaDoc, obri l'aplicació de correu, i envia les ofertes a l'encarregat de l'ajuntament.

Conclusions:

De l'estudi dels escenaris d'ús, es detecta que una funcionalitat no contemplada i que augmentaria la productivitat de l'aplicació, seria la possibilitat d'adjuntar automàticament un fitxer signat a un nou missatge de correu electrònic, des de la pròpia aplicació.
No sé si tindré temps d'implementar aquesta funcionalitat en aquesta versió, però queda com a prioritària en la llista d'ampliacions pendents. [1]

2.3.2 Fluxos d'interacció

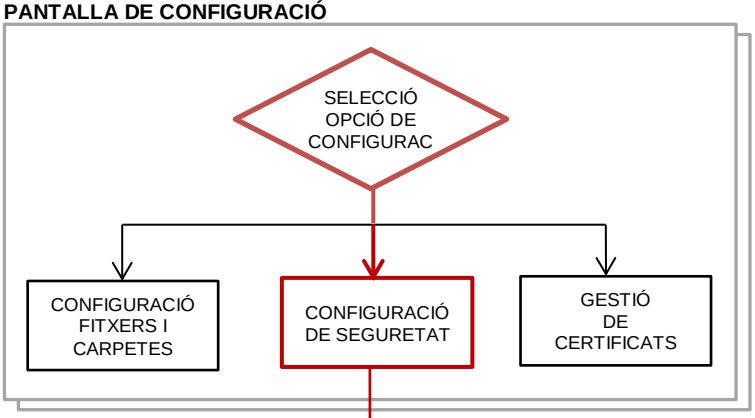
Configuració de l'aplicació: Registre de la carpeta de documents pendents



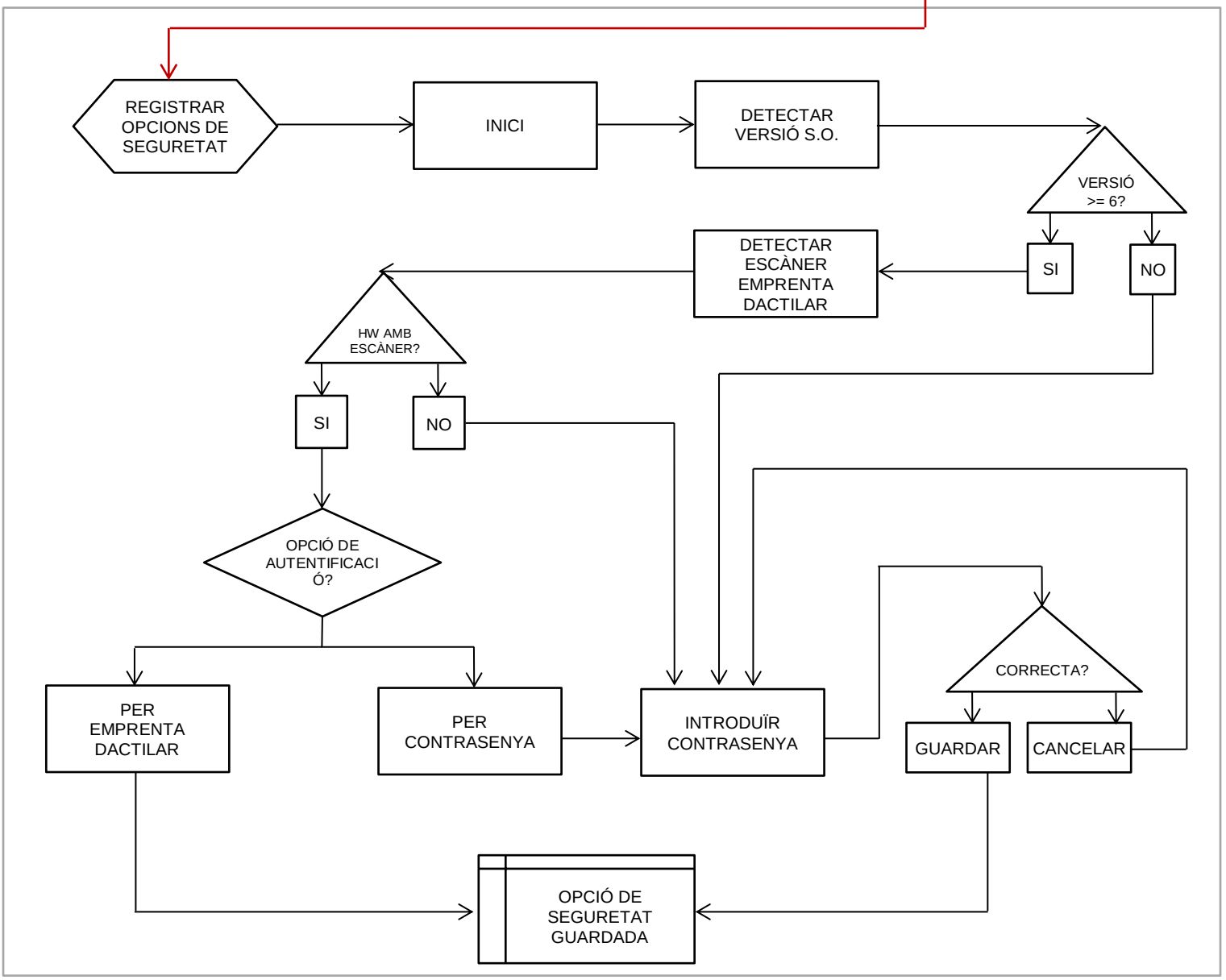
[1] Per a la confecció d'aquests escenaris d'ús he consultat el llibre *Simplemente pregunta: Integración de la accesibilidad en el diseño a la web http://www.uiaccess.com/justask/es* (6)

Configuració de l'aplicació: Configuració de la seguretat

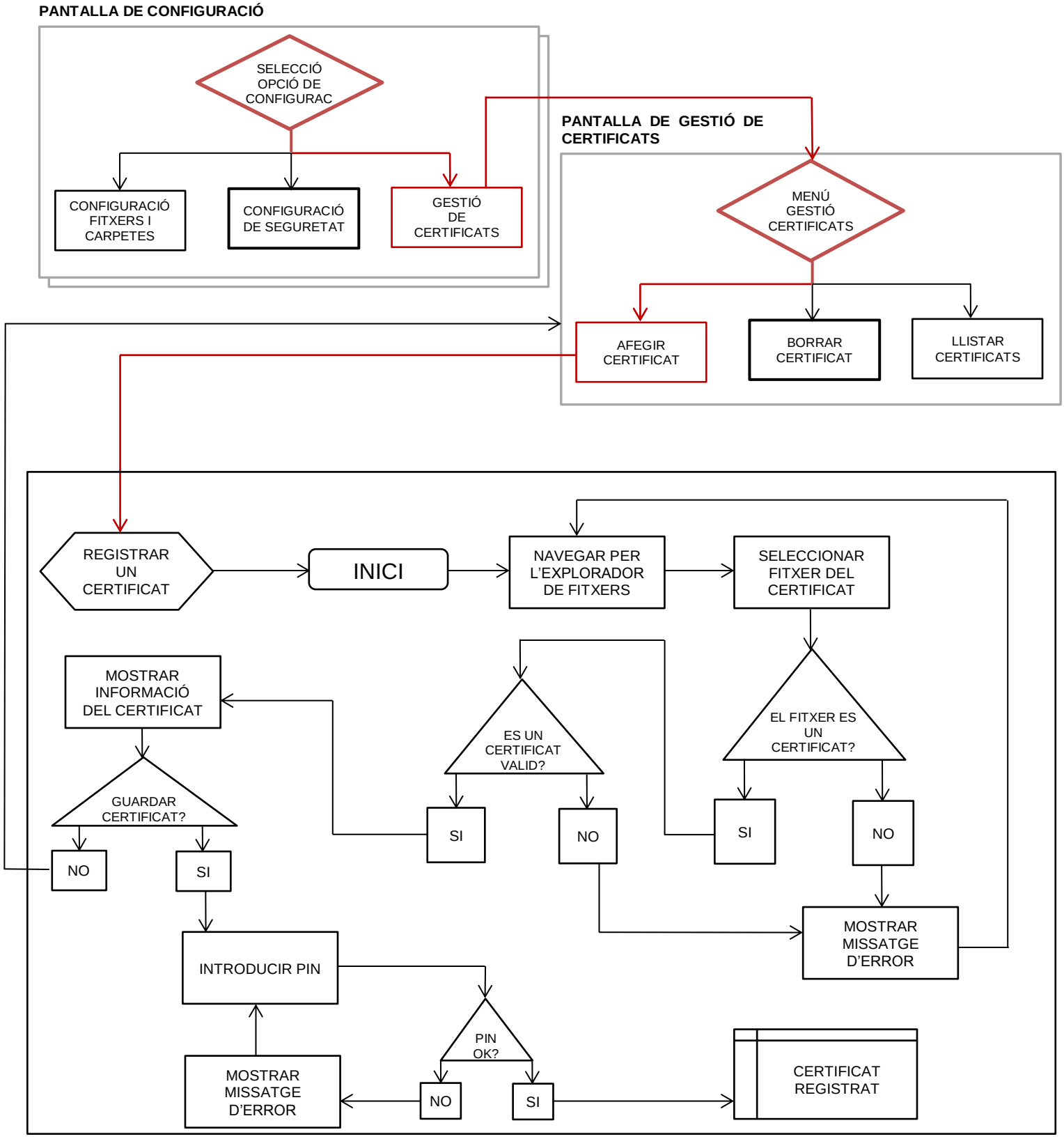
PANTALLA DE CONFIGURACIÓ



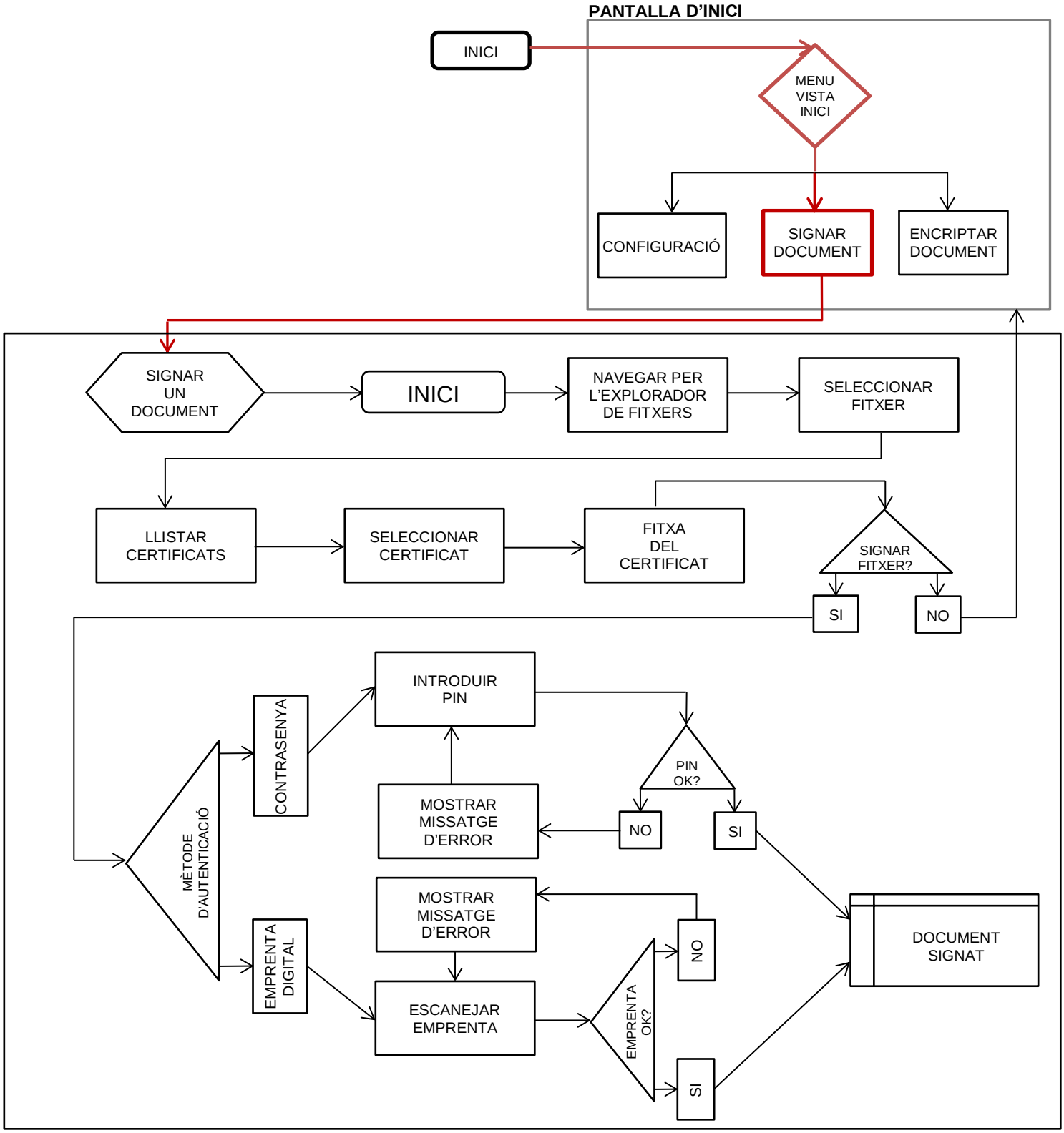
PROCÉS PER A LA SELECCIÓ DE LA OPCIÓ DE AUTENTIFICACIÓ



Configuració de l'aplicació: Registrar un certificat



Signar un document



2.4 Prototipatge

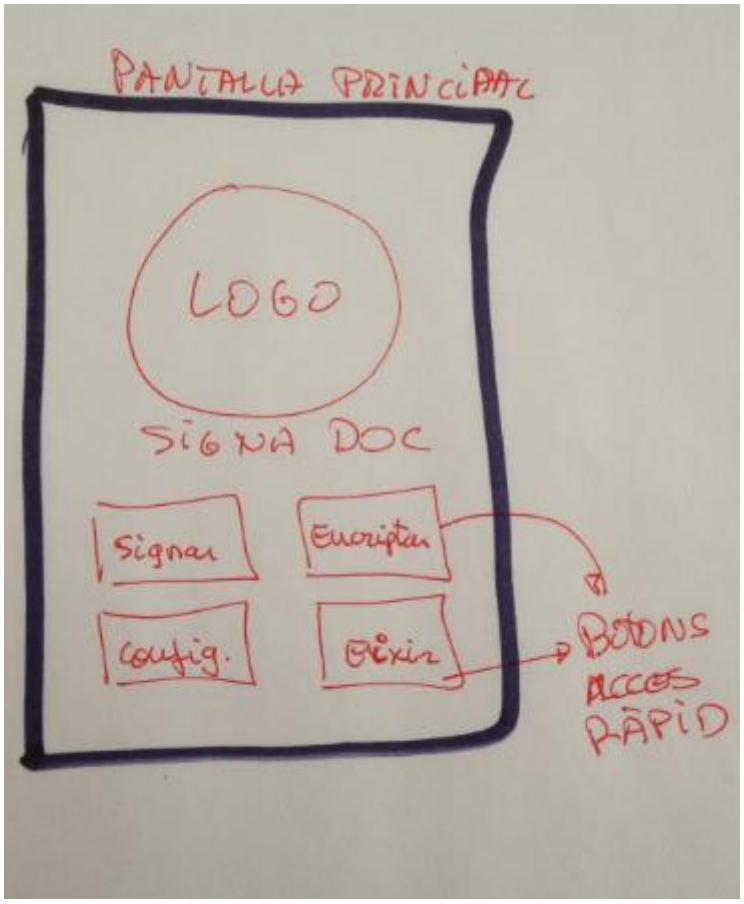
Una vegada realitzats els fluxos d'interacció, anem a començar amb el prototipat de l'aplicació.

En primer lloc començarem amb els Sketch, que són esbossos a mà alçada de les pantalles que conformaran l'aplicació.
L'objectiu d'aquests esbossos és reflectir la idea general del projecte i anar definint la interfície d'usuari, prenent decisions de disseny, com per exemple, on està la zona de navegació, com mostrar missatges a l'usuari, pantalles d'error,....

En la segona fase, partint dels Sketch, realitzarem un prototip d'alta definició, en el qual anirem definint el sistema de navegació entre pantalles, la paleta de colors aplicada, la iconografia, ..., alhora que podem interactuar amb ell, la qual cosa ens serveix per identificar, a partir de proves d'usuari, que àrees cal millorar, canviar o fins i tot eliminar.

2.4.1 Sketches

Pantalla d'inici



La pantalla d'inici, constarà d'un logo que ens ajudi a identificar visualment l'aplicació entre el conjunt d'apps que tenim instal·lades en el nostre smartphone, el nom i 4 botons d'accés ràpid. Dos per a les funcionalitats de signatura i encriptació, un altre per al de configuració i l'últim per a tancar l'aplicació

Figura 9: Sketch – Pantalla d'inici

Configuració de l'aplicació: Registre de la carpeta de documents pendents

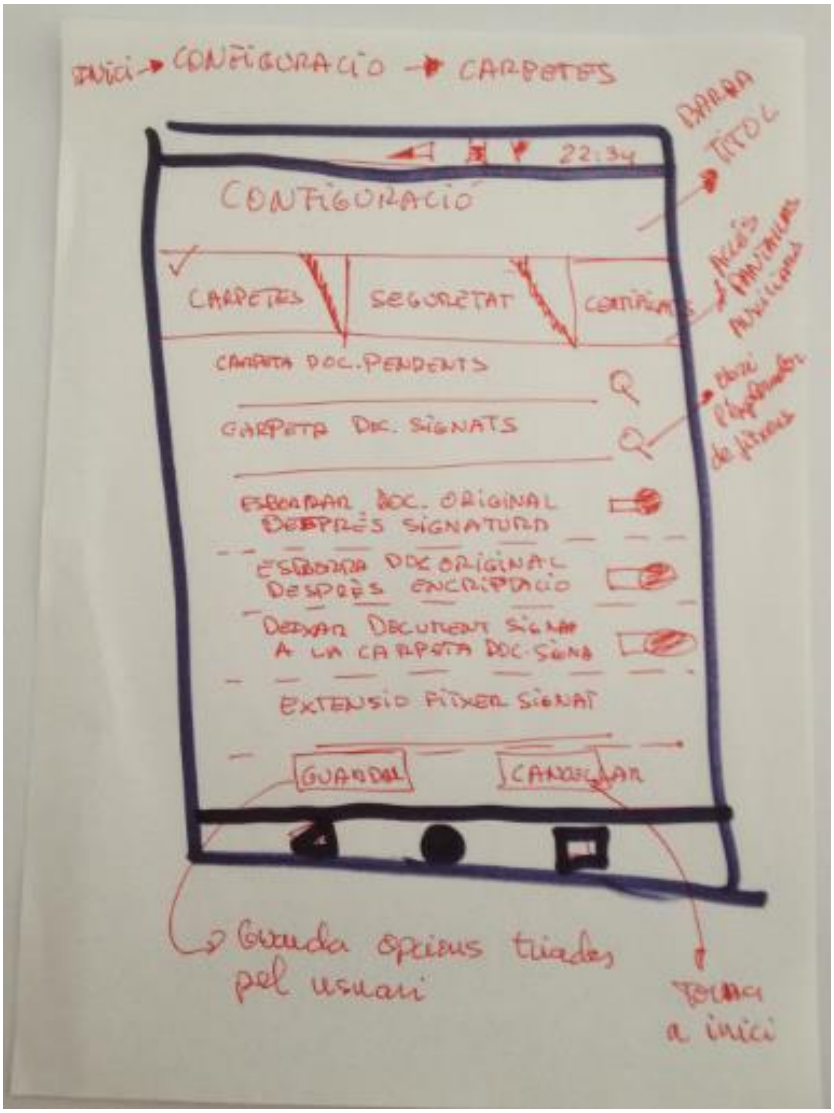
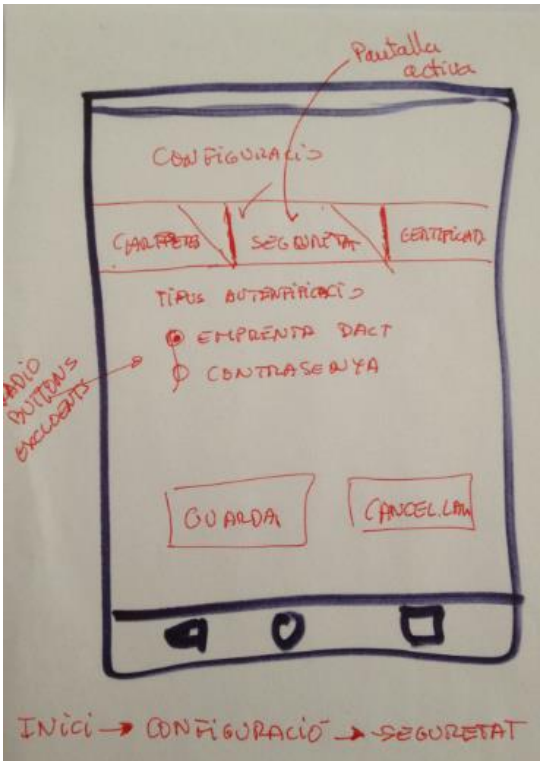


Figura 10: Sketch – Pantalla de configuració de opcions de carpetes i fitxers

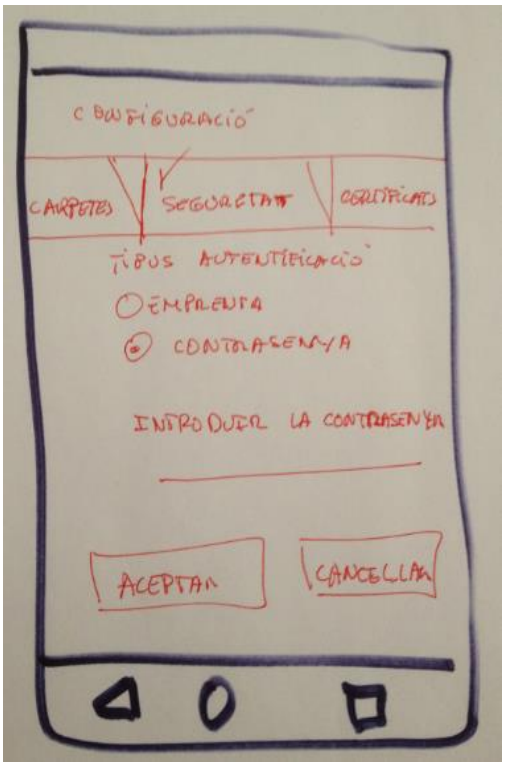
La pantalla de configuració disposa d'una barra de títol, per a indicar-nos en què pantalla ens hem situat, seguida d'una barra amb tres pestanyes, que ens permetran navegar entre les 3 pantalles de configuració: configuració d'opcions de carpeta i fitxers, configuració de la seguretat i gestió de certificats digitals.
La pantalla que per defecte ix quan entrem en configuració és la d'opcions de carpetes i fitxers. En ella podrem configurar les nostres preferències per a treballar amb els documents.

Configuració de l'aplicació: Configuració de la seguretat



Quan ens desplacem a la pantalla de seguretat, en primer lloc ens apareix un parell de botons de radi per a triar el tipus de seguretat que desitgem. L'opció seleccionada per defecte es l'opció d'Empremta dactilar.
En la part d'a baix es mostren els botons d'Acceptar i Cancel·lar

Figura 11: Sketch – Pantalla de seguretat amb empremta



Si seleccionem l'opció de Seguretat per Contrasenya, l'aplicació ens mostrarà dos quadres de text perquè la introduïm.
En la part d'a baix es mostren els botons d'Acceptar i Cancel·lar.

Figura 12 Sketch – Pantalla de seguretat amb contrasenya

Configuració de l'aplicació: Registrar un certificat

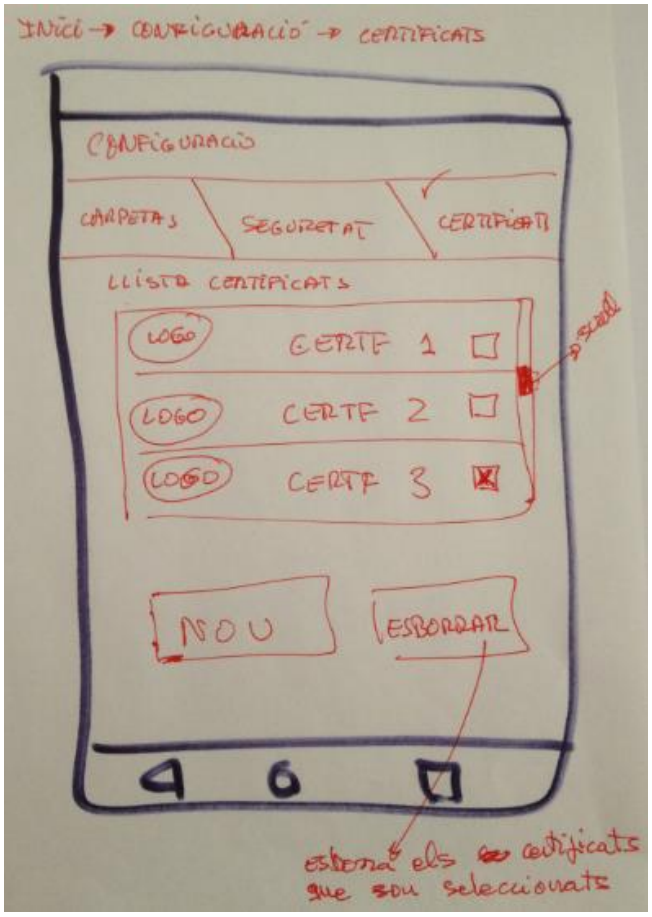


Figura 13 *Sketch – Pantalla de gestió de certificats*

La pantalla de gestió de certificats, mostra una llista dels certificats registrats en l'aplicació. Cada element de la llista conté un check per a poder seleccionar-ho, l'emissor i el logo de l'emissor.
En la part d'a baix tenim els botons de Nou o Esborrar. El botó d'esborrar, esborrarà els certificats que estiguen seleccionats.

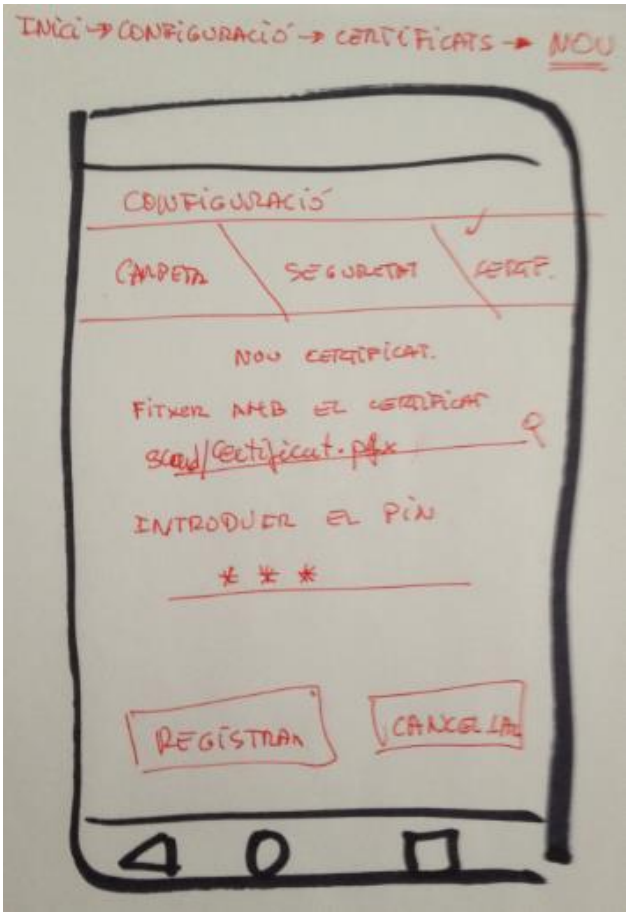


Figura 14: Sketch – Pantalla per a registrar un nou certificat

En la pantalla per a registrar un nou certificat, té un camp de text per a posar el nom del fitxer que conté el certificat (Es podrà seleccionar el fitxer amb el explorador de fitxers), i un altre on introduir el PIN. En la part d'a baix, els botons de Registrar, que registrarà el certificat en l'aplicació i el de Cancel·lar

Figura 15: Sketch – Pantalla de confirmació de registre d'un nou certificat

L'acció anterior ens portarà a aquesta pantalla si tot és correcte. Aquesta és la pantalla de confirmació de registre del certificat. Té un missatge per a l'usuari i un botó d'Acceptar, per a tornar a la pantalla d'inici.

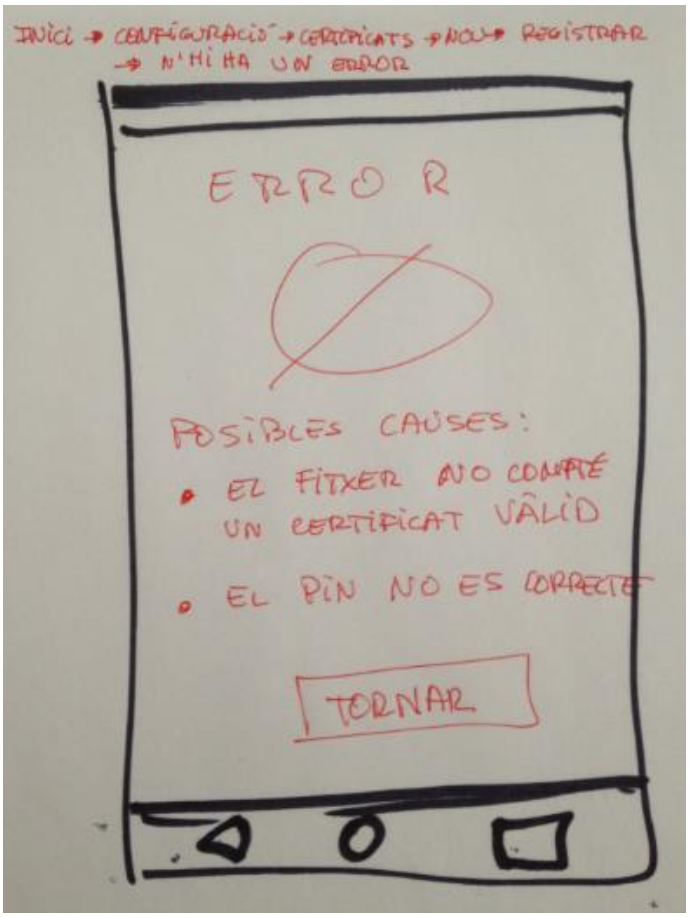


Figura 16: Sketch – Pantalla de error en el registre d'un nou certificat

L'acció anterior ens portarà a aquesta pantalla si alguna cosa no és correcte. Aquesta és la pantalla d'error en el registre del certificat. Té un missatge per a l'usuari i un botó d'Acceptar, per a tornar a la pantalla d'inici.

Signar un document

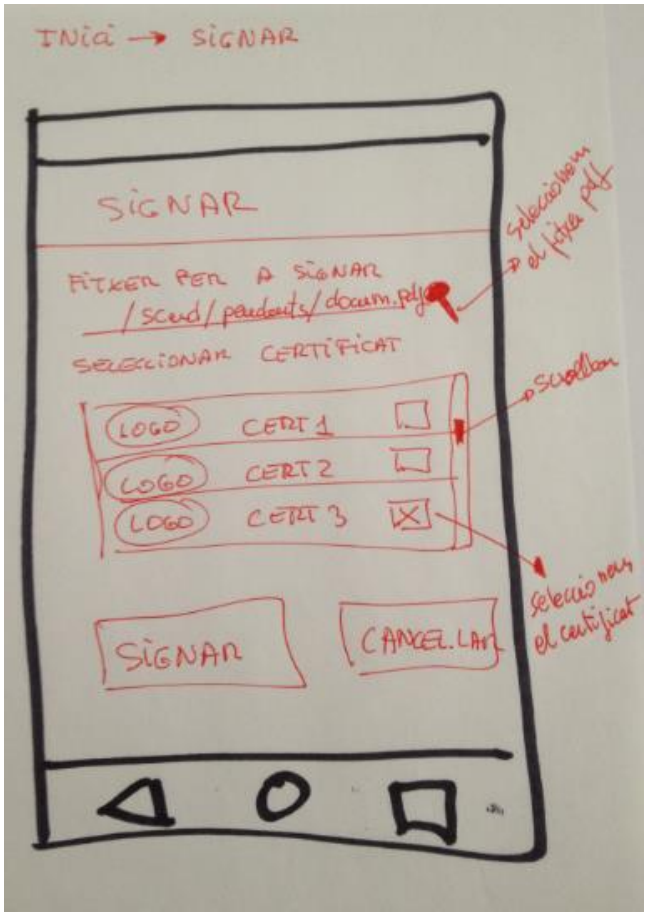


Figura 17: Sketch – Pantalla per a signar documents

Figura 18: Sketch – Pantalla de seguretat per a signar documents

La pantalla per a signar documents, consta d'una barra de títol, per a indicar-nos en què part de l'aplicació ens trobem, a continuació un camp de text per a posar el nom del document que volem signar, una llista dels certificats que tenim registrats en el sistema, amb un quadre de *check per a poder seleccionar el que volem utilitzar, i dos botons en la part d'a baix, el de Signar i el de Cancel·lar.

Una vegada seleccionat el document i el certificat, en prémer el botó de signar, l'aplicació ens mostrarà la pantalla de seguretat, en la qual hem d'escanejar la nostra petjada o introduir el PIN, d'acord a la configuració que tinguem.

Conté un missatge per a l'usuari indicant-li que acció ha de realitzar, i un botó de Cancel·lar.

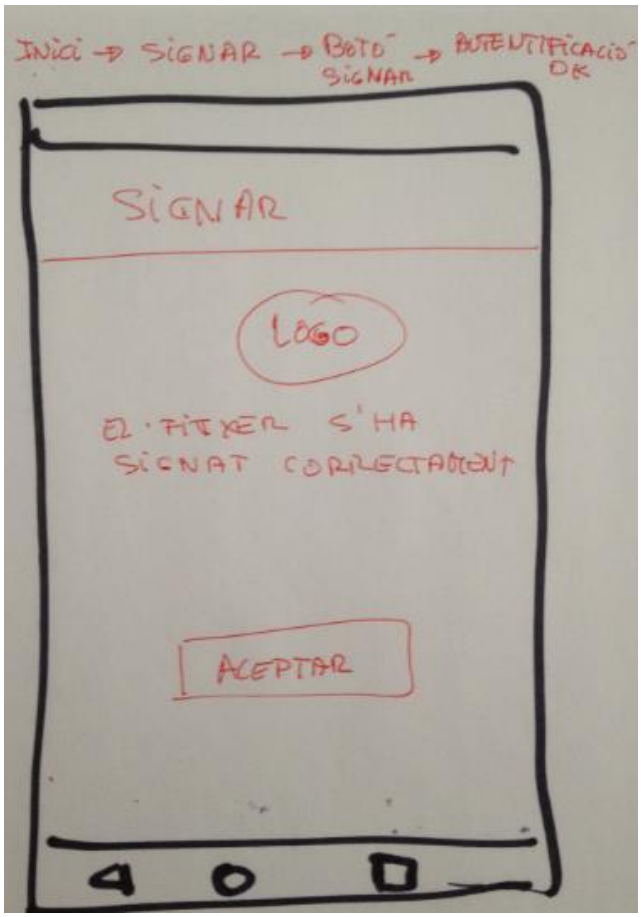


Figura 19: Sketch – Pantalla de confirmació de la signatura correcta d'un fitxer

L'acció anterior ens portarà a aquesta pantalla si tot és correcte. Aquesta és la pantalla de confirmació de que el document ha segut signat. Té un missatge per a l'usuari i un botó d'Acceptar, per a tornar a la pantalla d'inici.

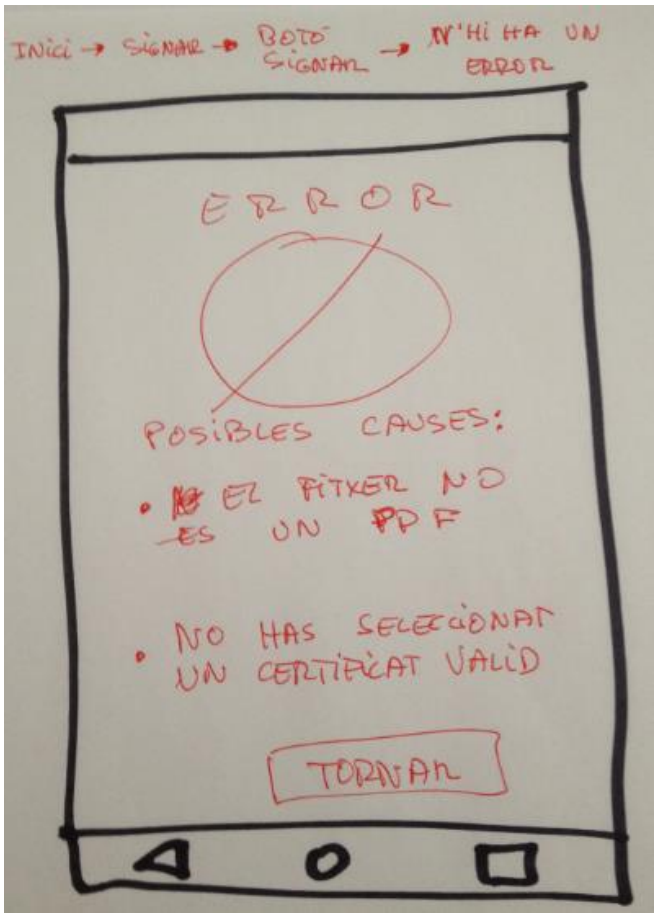


Figura 20: Sketch – Pantalla d'error a la signatura d'un document

L'acció anterior ens portarà a aquesta pantalla si alguna cosa no és correcta. Aquesta és la pantalla d'error en el procés de signatura del document. Té un missatge per a l'usuari i un botó d'Acceptar, per a tornar a la pantalla d'inici

2.4.2 Prototipus d'alta fidelitat

Pantalla d'inici

El prototip d'alta fidelitat interactiu s'ha realitzat amb l'aplicació JUSTINMIND, i pot ser visualitzat en la següent URL:

https://www.justinmind.com/usernote/tests/19626126/19626136/19626138/index.html

Figura 21: Prototipus d'alta fidelitat - Pantalla d'inici

Configuració de l'aplicació: Registre de la carpeta de documents pendents

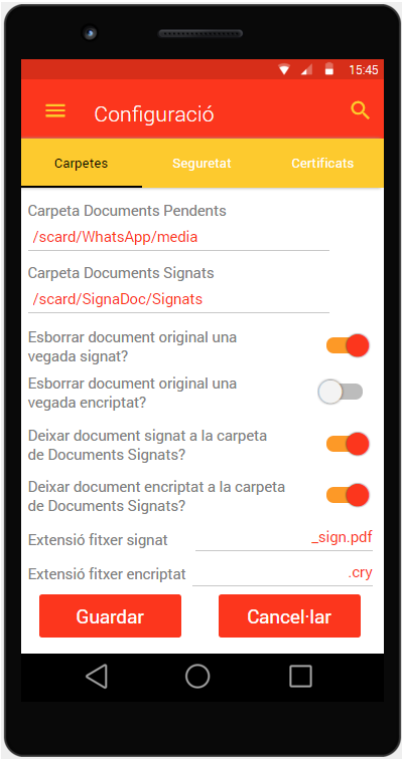


Figura 22: Prototipus d'alta fidelitat - Pantalla de configuració de carpetes i fitxers

Configuració de l'aplicació: Configuració de la seguretat

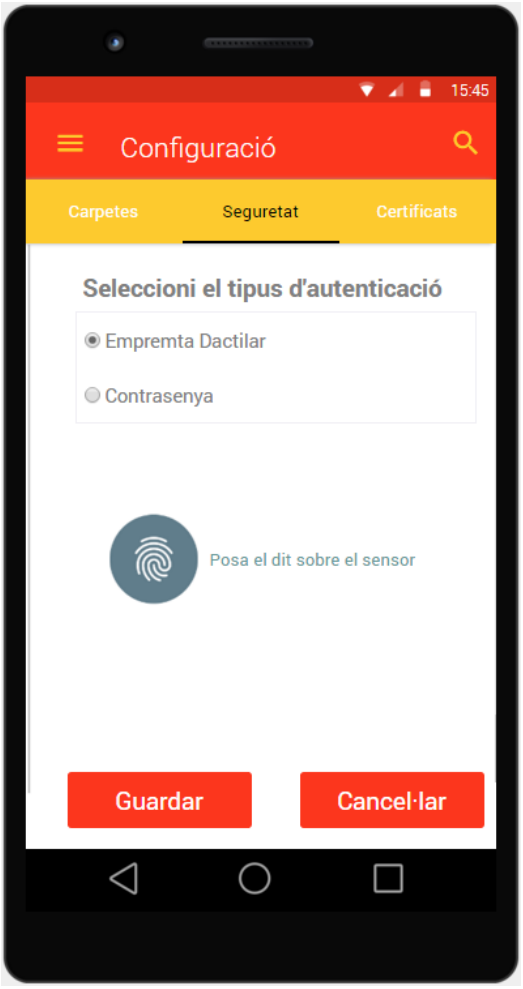


Figura 23: Prototipus d'alta fidelitat - Pantalla d'autenticació per empremta

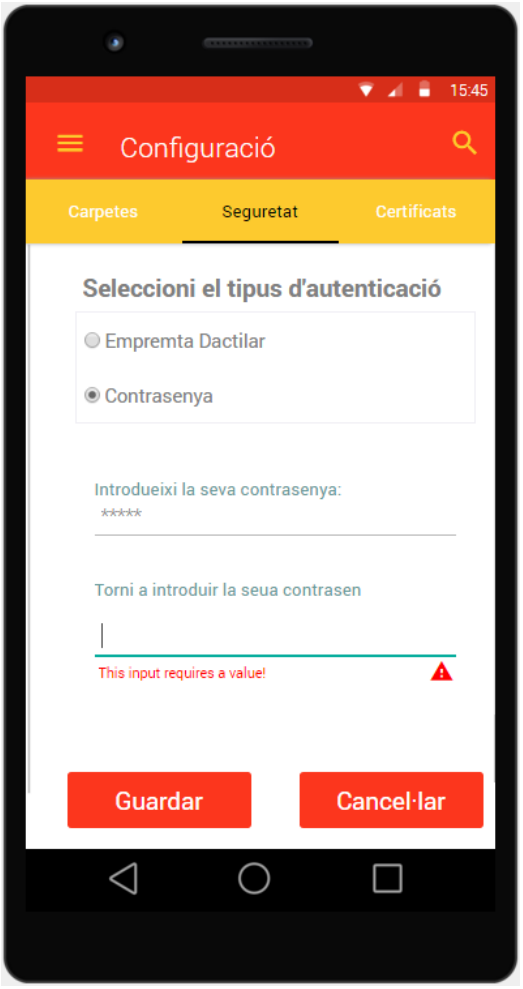


Figura 24: Prototipus d'alta fidelitat - Pantalla d'autenticació per contrasenya

Configuració de l'aplicació: Registrar un certificat

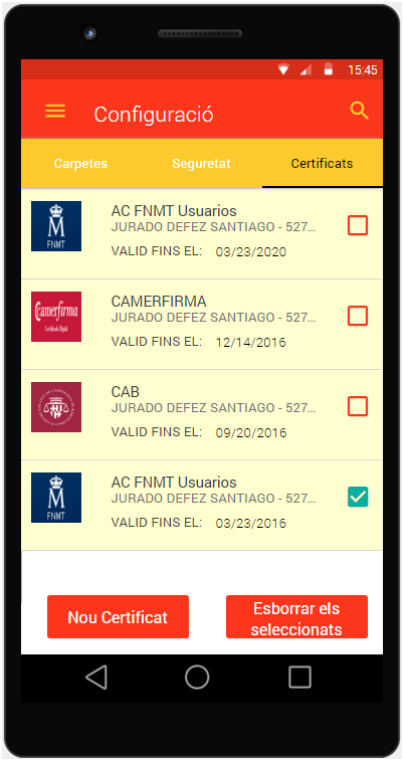


Figura 25: Prototipus d'alta fidelitat – Pantalla de configuració de certificats

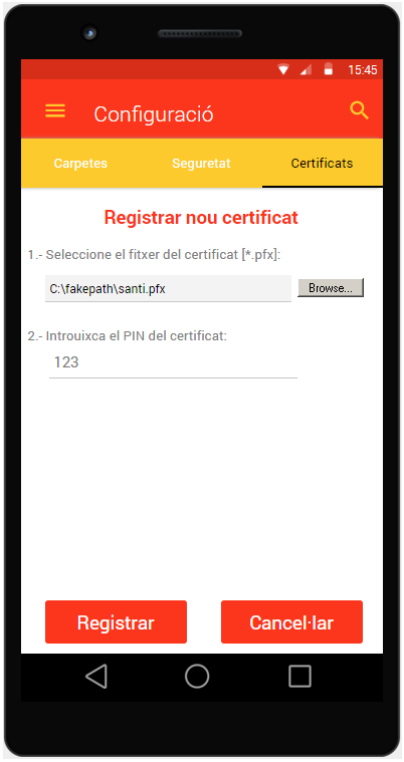


Figura 26: Prototipus d'alta fidelitat – Pantalla per a registrar un nou certificat digital

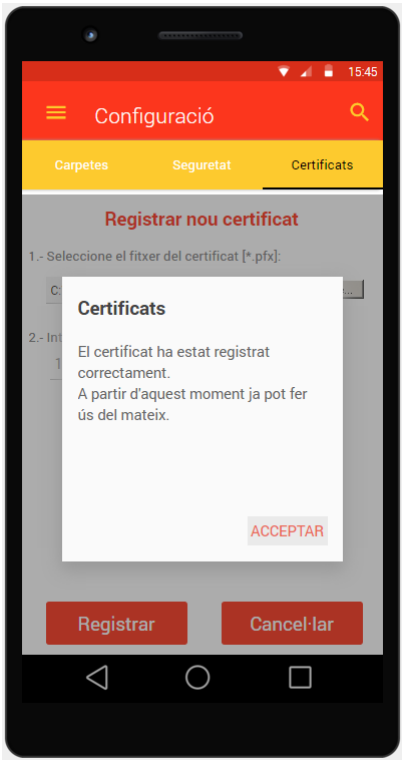


Figura 27: Prototipus d'alta fidelitat – Pantalla de confirmació de registre del certificat

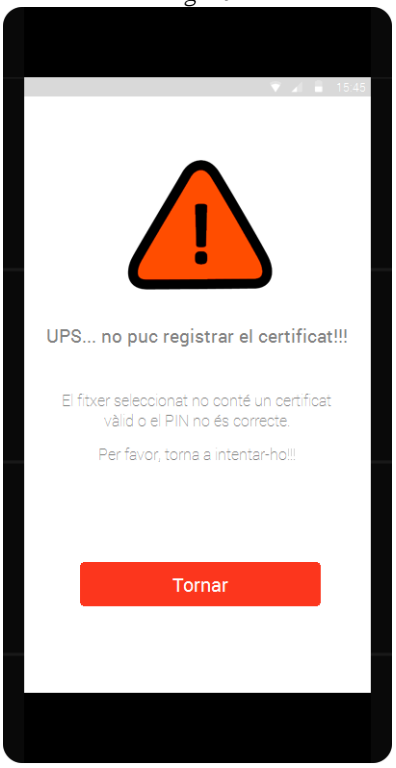


Figura28: Prototipus d'alta fidelitat – Pantalla de error en intentar registrar un nou certificat

Signar un document

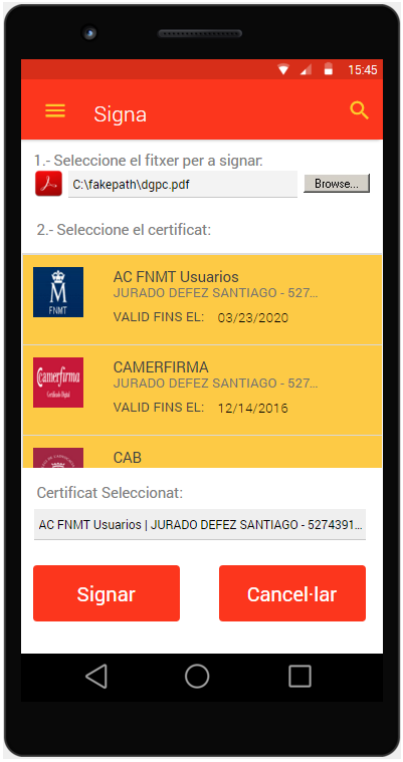


Figura 29: Prototipus d'alta fidelitat – Pantalla de Signar documents

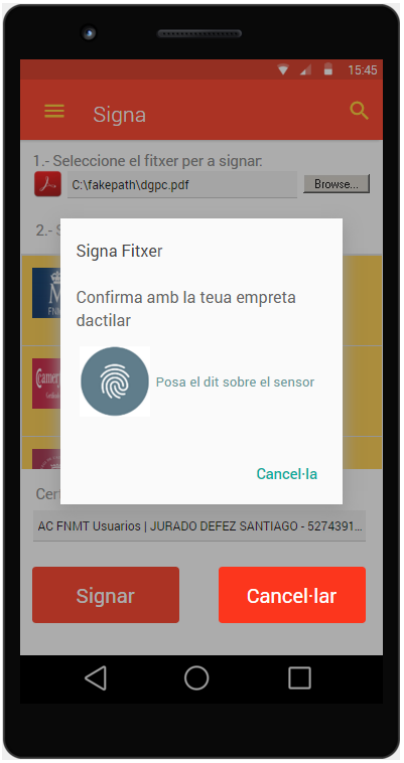


Figura 30: Prototipus d'alta fidelitat – Pantalla de sol·licitud de autenticació

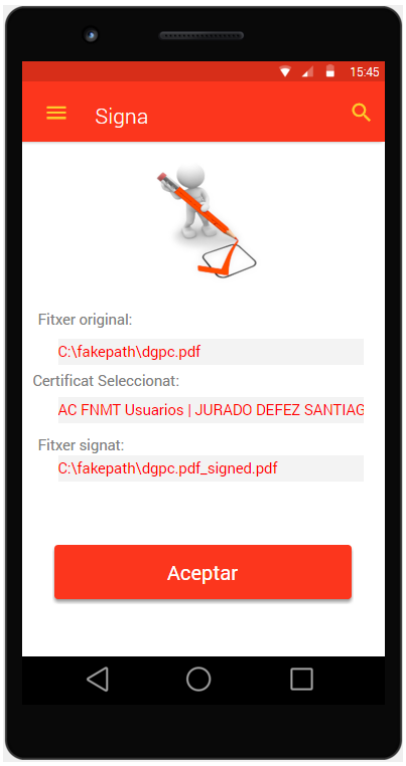


Figura 31: Prototipus d'alta fidelitat – Pantalla de confirmació de signatura del fitxer

Figura 32: Prototipus d'alta fidelitat – Pantalla de error en el procés de signatura

2.5 Avaluació

El test d'usuari del prototip es realitzarà, assignant-los tasques relacionades amb els escenaris i funcionalitats detectades als apartats anteriors i emplenant un qüestionari que ens ajudarà a detectar les àrees de millora en l'aplicació, després de la seva anàlisi.

El Test consta de tres seccions:

1. Pre-tasca: Les preguntes d'aquesta secció solen ser generals sobre certes habilitats de l'usuari i sol aprofitar-se per recollir informació útil sobre el perfil de l'usuari.
   Contindrà les següents preguntes:
   - Preguntes generals: Preguntes que ajuden a establir el perfil d'usuari i el seu lloc dins de la població en estudi. Inclou qüestions com a edat, sexe, ocupació, lloc de residència, aficions, estudis, aficions, etc.
   - Preguntes sobre Identitat: Les preguntes en aquest àmbit busquen establir si el lloc aconsegueix transmetre com és la seva funció principal. Per això, les preguntes s'enfoquen especialment a determinar si a primera vista l'usuari ha entès perquè serveix l'aplicació.

2. Post-tasca: Aquesta secció es repetirà tantes vegades com a tasques hagi de resoldre l'usuari.
   Contindrà les següents preguntes:
   - Preguntes sobre Contingut: Les preguntes d'aquesta secció i de les següents, s'han de fer després de permetre a l'usuari navegar per prototipus. El seu objectiu és determinar si la forma de presentar el contingut li permet a l'usuari fer-se una idea concreta de la funció que se li està oferint.
   - Preguntes sobre Navegació: Les preguntes d'aquesta secció permeten establir si la forma d'organitzar les pantalles en l'app és adequada d'acord a l'experiència, coneixements i expectatives que tingui l'usuari.

3. Post-test: Aquesta secció recollirà aspectes generals sobre la percepció de l'usuari després de la consecució de les diferents tasques plantejades.
   Contindrà les següents preguntes:
   - Preguntes sobre Aspecte visual: El color i l'aspecte visual és una eina important i essencial per potenciar el nostre projecte. Amb ells expressem sentiments, expectatives, desitjos .... Els desenvolupadors hem de buscar consell en l'usuari destinatari del nostre producte.
   - Preguntes sobre Utilitat: Les preguntes d'aquesta secció són les finals de la prova i tenen l'objectiu d'establir una espècie de resum general de l'experiència d'usuari.

Conclusions:: Aquesta prova permetrà determinar quins són les tasques més difícils de completar per part dels usuaris, així com els elements que siguin menys comprensibles. Aquesta informació haurà de ser avaluada i prioritzada amb l'objectiu de fer una llista de tasques que permeti fer les correccions que millor recolzin la capacitat de l'aplicació per ser usable.

Tasques a realitzar pels usuaris

Posarem als usuaris front a tres escenaris diferents, per a avaluar la usabilitat del prototipus.

Escenari 1

> "El teu certificat de la FNMT caduca dins d'un mes i has procedit a la seva renovació. Al moment que t'ho has descarregat de la web de la FNMT, el certificat anterior ha quedat cancel·lat, per la qual cosa has de registrar en l'app el nou certificat".
>
> *Nota per a l'usuari: la carpeta on s'obre per defecte el navegador de fitxers, té entre uns altres, un fitxer amb un certificat valgut. El prototip acceptarà qualsevol pin que s'introdueixi. El test finalitza quan es visualitzi la pantalla de verificació de certificat registrat correctament.*

Escenari 2

> "L'empresa on treballes té la seu a Barcelona, però el teu centre de treball està a València. L'empresa t'ha contractat fa 3 mesos i com has superat el període de prova, t'han ofert un contracte d'un any. El departament de recursos humans t'ha enviat el contracte per correu electrònic, per la qual cosa has de descarregar-ho i signar-ho amb el teu certificat digital, per a continuació retornar-ho al departament de RR.HH."
>
> *Nota per a l'usuari: la carpeta on s'obre per defecte el navegador de fitxers, té entre uns altres, un fitxer amb el contracte. Per simular l'escanejo de l'empremta dactilar, has de clickar sobre el logo de la empremta, en la pantalla corresponent. El test finalitza quan es visualitzi la pantalla de verificació de signat correcte.*

Escenari 3

> "Ets un usuari ocasional de l'app i quan la vas instal·lar en el teu nou Galaxy S6, el vas configurar perquè t'autentiqués amb l'empremta dactilar en utilitzar els certificats digitals. Ara, no saps perquè, el escàner no funciona correctament, per la qual cosa has decidit canviar el mètode d'autenticació per la introducció d'un PIN."
>
> *Nota per a l'usuari: El test finalitza quan hagis canviat l'opció de seguretat de "Empremta dactilar" a "Introducció d'una Contrasenya".*

Qüestionaris:

A continuació es presenten els qüestionaris que han d'emplenar els usuaris que realitzin el test, i que estan organitzats d'acord a l'exposat anteriorment.[2]

[2] Aquests qüestionaris han estat adaptats dels que apareixen en el document "Modelo de Test de Usuario" (7)

Presentació de l'Usuari

GENERAL

1.- Indiqui el seu nom?

2.- A què es dedica [Professió, Activitat]?

3.- Que experiència té en l'ús de smartphones?. Si té un, indiqui el sistema operatiu que utilitza (Android, IOS, Windows, ...)

4.- Utilitza apps en el mòbil habitualment?, Quantes hores ho utilitza al dia, a la setmana? Inclogui el nombre d'hores que utilitza el correu electrònic.

Si
No
N° d'hores: _____

5.- Què apps utilitza habitualment?

6.- Quan desitja trobar realitzar alguna tasca amb el seu smartphone, com troba una app que li doni aquesta funcionalitat?

7.- Abans de descarregar una app en el seu mòbil, que té en compte?

8.- Li importen les opinions d'altres usuaris abans de decidir-se per una app? o prefereix provar-la sense estar condicionat per altres opinions?

9.- Utilitza apps de pagament? Si és així, indiqui-les

Qüestionari 1

Aquestes preguntes s'han de fer quan l'usuari està mirant la pantalla inicial i abans de començar a navegar o fer "clic" sobre qualsevol contingut.

IDENTITAT

1.- Hi ha algun element gràfic o de text que li hagi ajudat a entendre que empresa és la propietària de la app?

2.- Amb la informació que s'ofereix en pantalla d'inici, és possible saber què funcionalitats ofereix l'aplicació? Com ho sap?

3.- <Només si no va ser esmentat abans> Relaciona els colors predominants en la app amb l'empresa propietària?

4.- <Només si no va ser esmentat abans> Dels elements que mostra aquesta pantalla, hi ha alguna cosa que vostè crea que està fora de lloc, perquè no pertany a l'empresa que vostè identifica com a propietària?

5.- Distingeix alguna imatge que representi (logotip) a la institució? Creu que apareix en un lloc important dins de la pàgina? Pot llegir el nom de la institució? És clar?

6.- Cap a quin tipus d'audiència creu vostè que està dirigida la app? Per què?

7.- Si hagués de prendre contacte telefònic o enviar una carta tradicional a la institució o empresa propietària de la app, s'ofereix informació de nombres o adreces? Són útils com per fer aquesta tasca? Li va costar trobar aquesta informació?

Qüestionari 2

Aquestes preguntes s'han de fer després de la finalització de cadascuna de les taques, propostes en els escenaris.

CONTINGUT

1.- Els textos usats als enllaços i botons són suficientment descriptius del que s'ofereix a les pàgines cap a les quals s'accedeix a través d'ells?

2.- En cas que se sol·licités algun arxiu adjunt, va ser fàcil saber el seu tipus o format? Li va ajudar la informació oferta per l'app sobre aquests arxius? O no va rebre cap informació?

3.- En cas d'error se li ha redirigit a una pantalla d'error?, va saber com va ser el motiu? Va poder tornar a la pantalla original fàcilmente? ho va poder esmenar?

4.- En manar dades mitjançant un formulari, l'app li avisa si els va rebre correctament o no?

5.- Ha estat fàcil i intuïtiu completar la tasca? quant temps li ha suposat?

NAVEGACIÓ

1.- Existeixen elements dins de les pantalles, que li permetin saber exactament on es troba i com tornar enrere?

2.- Com torna des de qualsevol pàgina del lloc a la pàgina d'inici? Veu alguna forma de fer-ho, que no sigui pressionant de tornada del telèfon? Li sembla clar?

3.- L'aplicació té diverses pantalles i Vostè ha ingressat i sortit de varis d'ells. La informació que se li ofereix en pantalla li sembla adequada per entendre on està situat a qualsevol moment? S'ha sentit perdut?

Qüestionari 3

Aquestes preguntes es realitzessin una vegada acabades les tasques proposades en els escenaris anteriors..

ASPECTE VISUAL

1.- Li va semblar adequada la forma en què es mostren les icones en l'aplicació?

2.- La paleta de colors li sembla adequada?

3.- Es va fixar si l'app tenia gràfiques amb animacions? Hi ha alguna que li hagi cridat l'atenció? Cap?

4.- Considera que gràficament l'app està equilibrada, molt simple o recarregat?

UTILITAT

1.- Després d'una primera mirada, li queda clar quin és l'objectiu de l'app? Quins serveis ofereix? Els pot enumerar?

2.- Creu que els serveis que s'ofereixen en aquest lloc són d'utilitat per al seu cas personal?

3.- Què és el que més et va cridar l'atenció positivament o negativament de la utilitat que ofereix l'app?

3. Disseny

3.1 Definició dels casos d'ús.

Configuració de preferències de carpetes i fitxers.

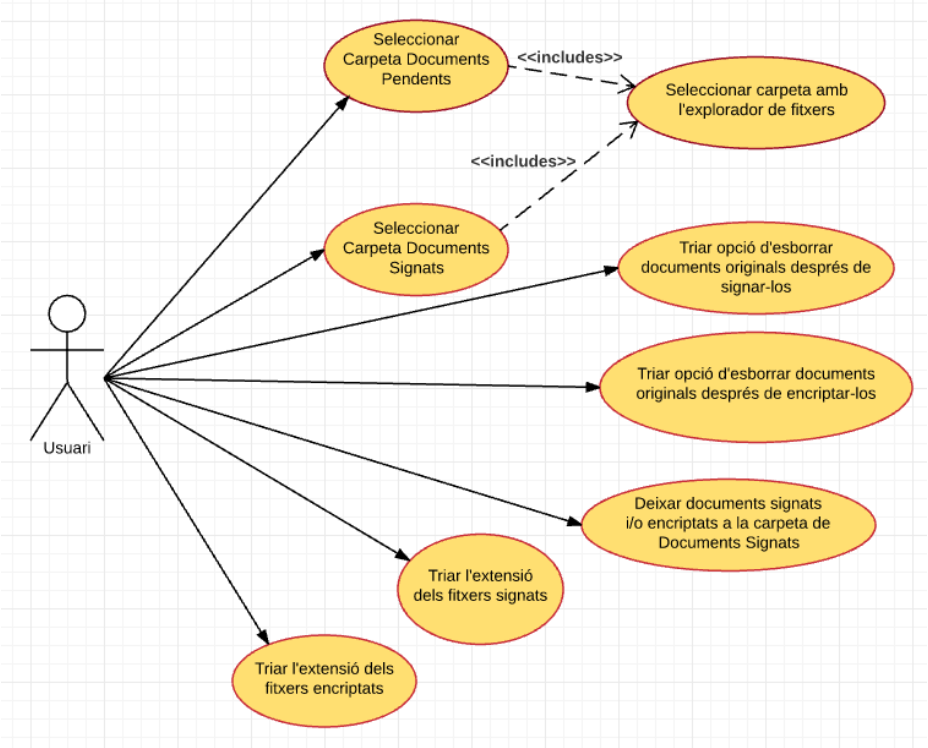


Figura 33: Cas d'us Configuració de preferències de carpetes i fitxers

Identificador:	CU-001		
Nom:	Configurar Ruta Carpeta Documents Pendents	Actors:	Usuari
Prioritat:	Normal	Iniciat per:	Usuari
Descripció:	El usuari pot configurar la ruta a una carpeta on deixi els documents pendents de signar. El sistema obrirà l'explorador de fitxers per aquesta carpeta quan es vulga signar o encriptar un document.		
Pre-condicions:			
Post-Condicions:	En acabar el cas d'ús la preferència de l'usuari estarà emmagatzemada en el sistema i la visualitzarà cada vegada que entre en la pantalla.		

Flux d'E vents	
Curs Normal	Alternatives
1. L'usuari selecciona la opció configuració en la pantalla principal	1. L'usuari ja està a la pantalla de Configuració de Carpetes y passa al punt 3
2. La pantalla de configuració apareix amb la pestanya de Carpetes seleccionada per defecte	
3. L'usuari selecciona la ruta a la carpeta de Documents Pendents, mitjançant l'ús de l'explorador de fitxers.	3.1 L'usuari cancel·la l'operació . 3.2 El sistema torna a la situació inicial prèvia a l'inici del cas d'ús
4 El sistema guarda la ruta seleccionada per l'usuari	
5. Finalitza el cas d'ús	

Identificador:	CU-002		
Nom:	Configurar Ruta Carpeta Documents Signats	Actors:	Usuari
Prioritat:	Normal	Iniciat per:	Usuari
Descripció:	El usuari pot configurar la ruta a una carpeta on l'aplicació deixarà els documents signats o encriptats.		
Pre-condicions:			
Post-Condicions:	En acabar el cas d'ús la preferència de l'usuari estarà emmagatzemada en el sistema i la visualitzarà cada vegada que entre en la pantalla.		

Flux d'E vents	
Curs Normal	Alternatives
1. L'usuari selecciona la opció configuració en la pantalla principal	1. L'usuari ja està a la pantalla de Configuració de Carpetes y passa al punt 3
2. La pantalla de configuració apareix amb la pestanya de Carpetes seleccionada per defecte	
3. L'usuari selecciona la ruta a la carpeta de Documents Signats, mitjançant l'ús de l'explorador de fitxers.	3.1 L'usuari cancel·la l'operació . 3.2 El sistema torna a la situació inicial prèvia a l'inici del cas d'ús
4 El sistema guarda la ruta seleccionada per l'usuari	
5. Finalitza el cas d'ús	

Identificador:	CU-003		
Nom:	Opció d'esborrar documents originals després de signar-los	Actors:	Usuari
Prioritat:	Normal	Iniciat per:	Usuari
Descripció:	El usuari pot configurar el comportament de l'aplicació una vegada ha signat un document.		
Pre-condicions:			
Post-Condicions:	En acabar el cas d'ús la preferència de l'usuari estarà emmagatzemada en el sistema i la visualitzarà cada vegada que entre en la pantalla. En el cas de activar l'opció el sistema esborrarà el document original després del procés de signatura.		

Flux d'E vents	
Curs Normal	Alternatives
1. L'usuari selecciona la opció configuració en la pantalla principal	1. L'usuari ja està a la pantalla de Configuració de Carpetes y passa al punt 3
2. La pantalla de configuració apareix amb la pestanya de Carpetes seleccionada per defecte	
3. L'usuari pot activar/desactivar l'opció de "Esborrar el document original una vegada ha sigut signat"	3.1 L'usuari cancel·la l'operació . 3.2 El sistema torna a la situació inicial prèvia a l'inici del cas d'ús
4 El sistema guarda la preferència de l'usuari	
5. Finalitza el cas d'ús	

Identificador:	CU-004		
Nom:	Opció d'esborrar documents originals després de encriptar-los	Actors:	Usuari
Prioritat:	Normal	Iniciat per:	Usuari

Descripció:	El usuari pot configurar el comportament de l'aplicació una vegada ha encriptat un document.
Pre-condicions:	
Post-Condicions:	En acabar el cas d'ús la preferència de l'usuari estarà emmagatzemada en el sistema i la visualitzarà cada vegada que entre en la pantalla. En el cas de activar l'opció el sistema esborrarà el document original després del procés d'encriptació.

Flux d'E vents	
Curs Normal	**Alternatives**
1. L'usuari selecciona la opció configuració en la pantalla principal	1. L'usuari ja està a la pantalla de Configuració de Carpetes y passa al punt 3
2. La pantalla de configuració apareix amb la pestanya de Carpetes seleccionada per defecte	
3. L'usuari pot activar/desactivar l'opció de "Esborrar el document original una vegada ha sigut encriptat"	3.1 L'usuari cancel·la l'operació . 3.2 El sistema torna a la situació inicial prèvia a l'inici del cas d'ús
4 El sistema guarda la preferència de l'usuari	
5. Finalitza el cas d'ús	

Identificador:	CU-005		
Nom:	Deixar documents signats o encriptats a la carpeta de Documents Signats	**Actors:**	Usuari
Prioritat:	Normal	**Iniciat per:**	Usuari
Descripció:	El usuari pot configurar el comportament de l'aplicació una vegada ha signat un document.		
Pre-condicions:	La ruta a la carpeta de Documents Signats no pot estar en blanc.		
Post-Condicions:	En acabar el cas d'ús la preferència de l'usuari estarà emmagatzemada en el sistema i la visualitzarà cada vegada que entre en la pantalla. En el cas de activar l'opció el sistema deixarà els documents signats en la ruta "Carpeta de Documents Signats", en cas contrari els deixarà en la mateixa carpeta que el document original.		

Flux d'E vents	
Curs Normal	**Alternatives**
1. L'usuari selecciona la opció configuració en la pantalla principal	1. L'usuari ja està a la pantalla de Configuració de Carpetes y passa al punt 3
2. La pantalla de configuració apareix amb la pestanya de Carpetes seleccionada per defecte	
3. L'usuari pot activar/desactivar l'opció de "Deixar documents signats a la carpeta Documents Signats"	3.1 L'usuari cancel·la l'operació . 3.2 El sistema torna a la situació inicial prèvia a l'inici del cas d'ús
4 El sistema guarda la preferència de l'usuari	
5. Finalitza el cas d'ús	

Identificador:	CU-006		
Nom:	Extensió fitxer signat	**Actors:**	Usuari
Prioritat:	Normal	**Iniciat per:**	Usuari
Descripció:	El usuari pot especificar l'extensió que tindrà el nou fitxer que conté el document signat		
Pre-condicions:	L'extensió per defecte serà *_sgnt.pdf		
Post-Condicions:	En acabar el cas d'ús la preferència de l'usuari estarà emmagatzemada en el sistema i la visualitzarà cada vegada que entre en la pantalla. El sistema nomenarà el fitxer resultant amb el següent patró: NomFitxerOriginalExtensió.		

Flux d'E vents

Curs Normal	Alternatives
1. L'usuari selecciona la opció configuració en la pantalla principal	1.1 L'usuari ja està a la pantalla de Configuració de Carpetes y passa al punt 3
2. La pantalla de configuració apareix amb la pestanya de Carpetes seleccionada per defecte	
3. L'usuari posa l'extensió de fitxer signat de la seua preferència	3.1 L'usuari cancel·la l'operació .
4 El sistema guarda la preferència de l'usuari	3.2 El sistema torna a la situació inicial prèvia a l'inici del cas d'ús
5. Finalitza el cas d'ús	

Identificador:	CU-007		
Nom:	Extensió fitxer encriptat	Actors:	Usuari
Prioritat:	Normal	Iniciat per:	Usuari
Descripció:	El usuari pot especificar l'extensió que tindrà el nou fitxer que conté el document signat		
Pre-condicions:	L'extensió per defecte serà *.cry		
Post-Condicions:	En acabar el cas d'ús la preferència de l'usuari estarà emmagatzemada en el sistema i la visualitzarà cada vegada que entre en la pantalla. El sistema nomenarà el fitxer resultant amb el següent patró: NomFitxerOriginalExtensió.		
Flux d'E vents			
Curs Normal		Alternatives	
1. L'usuari selecciona la opció configuració en la pantalla principal		1.1 L'usuari ja està a la pantalla de Configuració de Carpetes y passa al punt 3	
2. La pantalla de configuració apareix amb la pestanya de Carpetes seleccionada per defecte			
3. L'usuari posa l'extensió de fitxer encriptat de la seua preferència		3.1 L'usuari cancel·la l'operació .	
4 El sistema guarda la preferència de l'usuari		3.2 El sistema torna a la situació inicial prèvia a l'inici del cas d'ús	
5. Finalitza el cas d'ús			

Configuració de la seguretat.

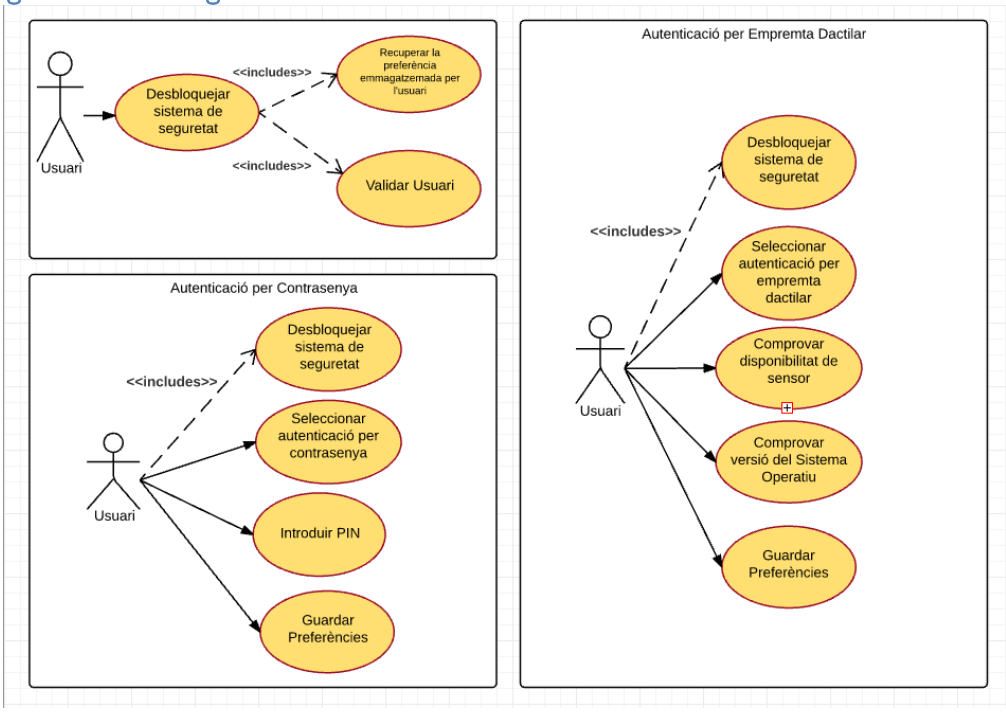


Figura 34: Cas d'ús de Configuració de la seguretat

Identificador:	CU-008		
Nom:	Desbloquejar sistema de seguretat	Actors:	Usuari
Prioritat:	Normal	Iniciat per:	Sistema
Descripció:	Per a realitzar canvis en les preferències del sistema de seguretat, cal desbloquejar el sistema, identificant-se d'acord a l'última preferència guardada		
Pre-condicions:			
Post-Condicions:	El sistema queda desbloquejat i l'usuari pot canviar les preferències de seguretat		
Flux d'E vents			
Curs Normal		Alternatives	
1. El sistema recupera la preferència de validació de l'usuari: Contrasenya o escaneig d'empremta dactilar		1.1 Es el primer ús i el sistema no té registrat cap preferència de validació. 1.2 El sistema passa al punt 3	
2. L'usuari es valida mitjançant contrasenya o empremta digital			
3. El sistema es desbloqueja			
4. Finalitza el cas d'ús			

Identificador:	CU-009		
Nom:	Configurar seguretat per empremta dactilar	Actors:	Usuari
Prioritat:	Normal	Iniciat per:	Sistema
Descripció:	Per a realitzar canvis en les preferències del sistema de seguretat, cal desbloquejar el sistema, identificant-se d'acord a l'última preferència guardada		
Pre-condicions:			
Post-Condicions:	El sistema queda desbloquejat i l'usuari pot canviar les preferències de seguretat		
Flux d'E vents			
Curs Normal		Alternatives	
1. L'usuari selecciona la opció configuració en la pantalla principal i a continuació la pestanya de seguretat			
2. Se desbloqueja el sistema de seguretat [CU-008]		2.1 N'hi ha un error en el procés de desbloqueig. 2.2 Es mostra un avís d'error a l'usuari 2.2 Finalitza el cas d'ús	
3. L'usuari selecciona l'opció de Autenticació per Empremta Dactilar			
4. El sistema comprova que el hardware conté un escàner d'empremtes dactilars		4.1 El hardware no es compatible. 4.2 El sistema mostra una pantalla informant de l'error a l'usuari. 4.3 Finalitza el cas d'ús	
5. El sistema comprova que la seua versió del sistema operatiu es compatible.		5.1 El S.O. no es compatible. 5.2 El sistema mostra una pantalla informant de l'error a l'usuari. 5.3 Finalitza el cas d'ús	
6. L'usuari escaneja la seua empremta			
7. Una pantalla de confirmació indica a l'usuari que el procés s'ha completat			
7. Finalitza el cas d'ús			

Identificador:	CU-010		
Nom:	Configurar seguretat per contrasenya	Actors:	Usuari
Prioritat:	Normal	Iniciat per:	Usuari
Descripció:	El usuari configura la seua preferència de autenticació per contrasenya		
Pre-condicions:			
Post-Condicions:	El sistema tindrà emmagatzemada la preferència de autentificació de l'usuari		

Flux d'E vents	
Curs Normal	Alternatives
1. L'usuari selecciona la opció configuració en la pantalla principal i a continuació la pestanya de seguretat	
2. Se desbloqueja el sistema de seguretat [CU-008]	2.1 N'hi ha un error en el procés de desbloqueig. 2.2 Es mostra un avís d'error a l'usuari 2.3 Finalitza el cas d'ús
3. L'usuari selecciona l'opció de Autenticació per Contrasenya	
4. L'usuari introdueix una contrasenya	
5. L'usuari confirma la contrasenya	5.1 L'usuari s'equivoca en introduir la contrasenya 5.2 El sistema mostra un avís d'error 5.3 El sistema torna al punt 5
6 L'usuari confirma els canvis	6.1. L'usuari cancel·la el procés 6.2 Finalitza el cas d'ús
7. Una pantalla de confirmació indica a l'usuari que el procés s'ha completat	
8. Finalitza el cas d'ús	

Gestió de Certificats.

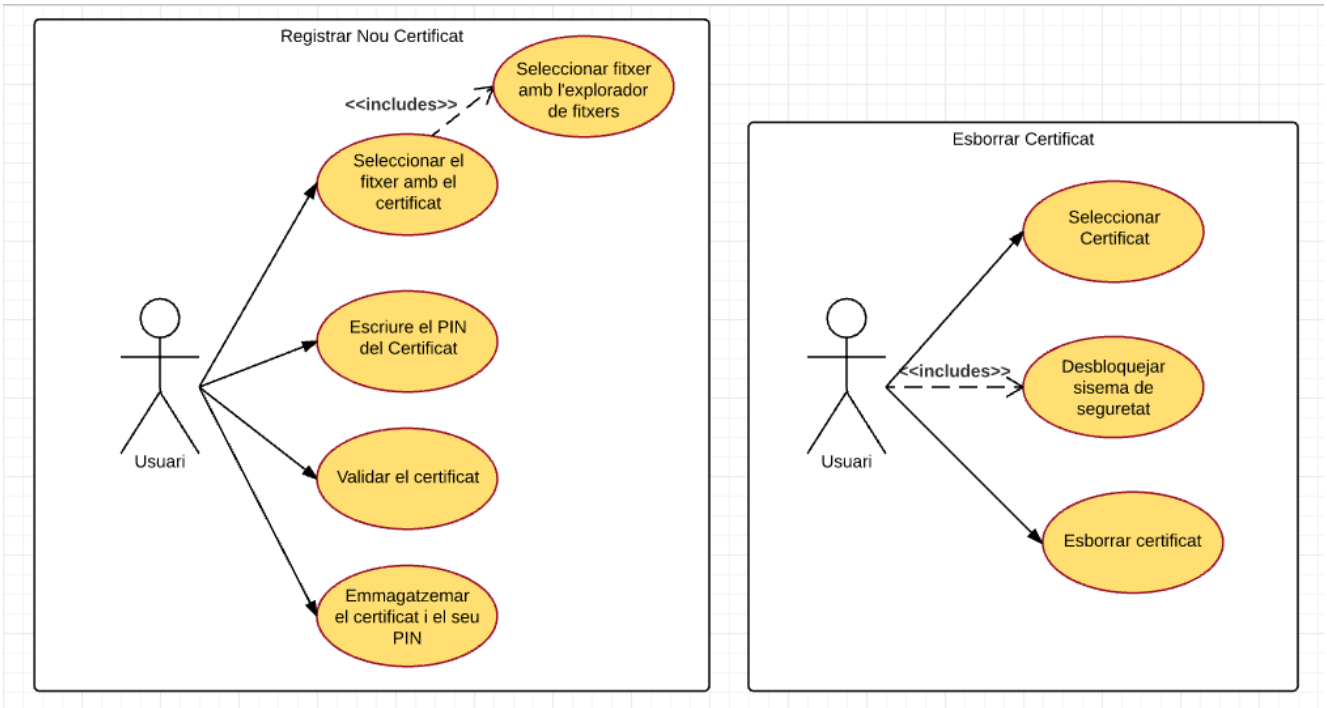


Figura 35: Cas d'ús de Gestió de Certificats

Identificador:	CU-011		
Nom:	Esborrar un certificat	Actors:	Usuari
Prioritat:	Normal	Iniciat per:	Usuari
Descripció:	El usuari esborra un certificat		
Pre-condicions:	El certificat deu d'estar registrat al sistema		
Post-Condicions:	El sistema no contindrà el certificat al magatzem de certificats		

Flux d'E vents	
Curs Normal	Alternatives
1. L'usuari selecciona la opció configuració en la pantalla principal i a continuació la pestanya de Certificats	
2. Selecciona el certificats de la llista	
3. Se desbloqueja el sistema de seguretat [CU-008]	3.1 N'hi ha un error en el procés de desbloqueig 3.2 Es mostra un avís d'error a l'usuari. 3.3 Finalitza el cas d'ús
5 L'usuari confirma els canvis	5.1. L'usuari cancel·la el procés 5.2 Finalitza el cas d'ús
7. Una pantalla de confirmació indica a l'usuari que el procés s'ha completat	
8. Finalitza el cas d'ús	

Identificador:	CU-012		
Nom:	Registrar un nou certificat	Actors:	Usuari
Prioritat:	Normal	Iniciat per:	Usuari
Descripció:	El usuari registra un nou certificat dins de l'App		
Pre-condicions:			
Post-Condicions:	El sistema afegirà el nou certificat al magatzem de certificats i guardarà el PIN associat		

Flux d'E vents	
Curs Normal	Alternatives
1. L'usuari selecciona la opció configuració en la pantalla principal i a continuació la pestanya de Certificats	
2. Selecciona l'opció de Nou Certificat	
3. L'usuari selecciona el fitxer que conté el certificat mitjançant l'explorador de fitxers	3.1 L'usuari selecciona un fitxer que no conté un certificat 3.2 El sistema mostra un avís d'error 3.3 El sistema torna al punt 3
4. L'usuari introdueix el PIN associat al certificat	
5. El sistema valida el certificat, obrint-ho amb el PIN i comprovant que no està caducat.	5.1 L'usuari s'equivoca en introduir el PIN 5.2 El sistema mostra un avís d'error 5.3 El sistema torna al punt 4
6 L'usuari confirma els canvis	6.1. L'usuari cancel·la el procés 6.2 Finalitza el cas d'ús
7. Una pantalla de confirmació indica a l'usuari que el procés s'ha completat	
8. Finalitza el cas d'ús	

Signar Document.

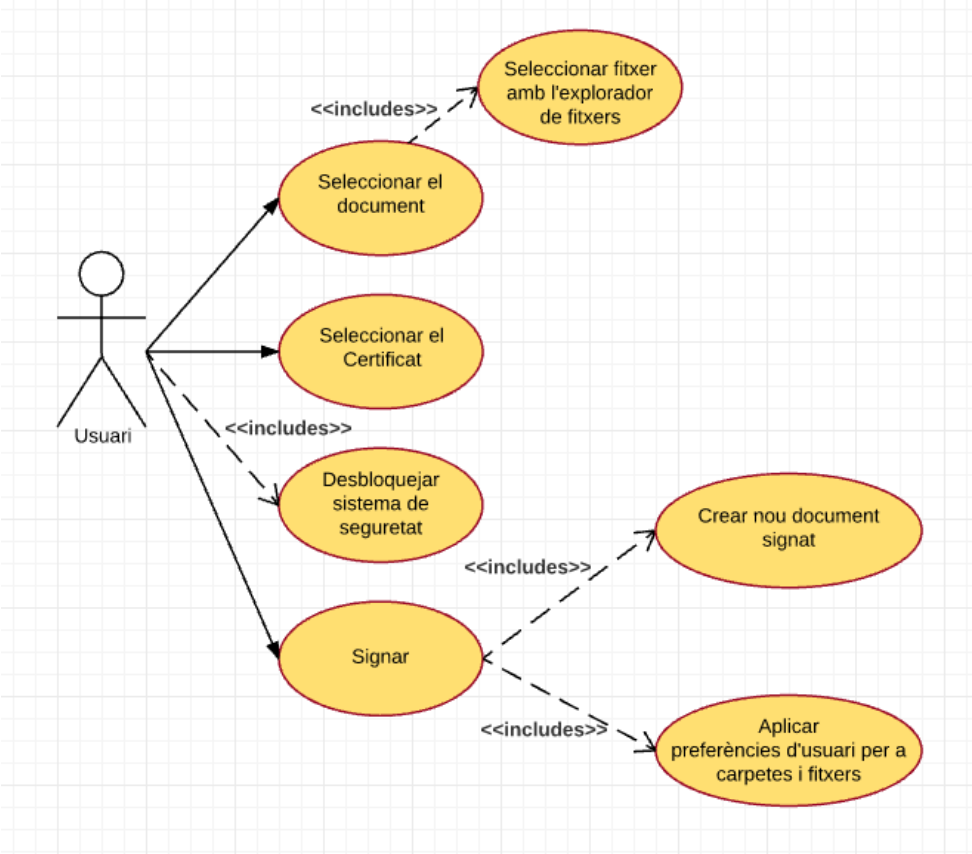


Figura 36: Cas d'ús per a Signar un Document

Identificador:	CU-013		
Nom:	Signar un document	Actors:	Usuari
Prioritat:	Normal	Iniciat per:	Usuari
Descripció:	El usuari signa un document		
Pre-condicions:	Ha d'haver-hi almenys un certificat registrat en el sistema		
Post-Condicions:	Es crearà un nou document amb el contingut de l'original i signat amb un certificat digital		

Flux d'E vents	
Curs Normal	Alternatives
1. L'usuari selecciona la opció Signar en la pantalla principal.	
2. L'usuari selecciona el fitxer que conté el document mitjançant l'explorador de fitxers	
3. Selecciona un certificats de la llista	
4. Se desbloqueja el sistema de seguretat [CU-008]	4.1 N'hi ha un error en el procés de desbloqueig. 4.2 Es mostra un avís d'error a l'usuari 4.3 Finalitza el cas d'ús
5 L'usuari confirma els canvis	5.1. L'usuari cancel·la el procés 5.2 Finalitza el cas d'ús
6. El sistema crea un document signat amb el certificat i	

amb el contingut de l'original.	
7. El sistema deixa el fitxer signat i amb el nom segons les preferències de l'usuari per a carpetes i fitxers.	7.1 Ocorre un error. Per exemple no hi ha espai en memòria per a emmagatzemar el nou fitxer. 7.2 Es mostra un avís d'error a l'usuari 7.3 Finalitza el cas d'ús
8. Una pantalla de confirmació indica a l'usuari que el procés s'ha completat	
8. Finalitza el cas d'ús	

3.2 Disseny de l'arquitectura

Persistència

En aquesta aplicació no farem ús de l'emmagatzematge en base de dades, però com quasi totes les aplicacions, sí que tenim la necessitat d'emmagatzemar informació en manera local.
Atenent a la funcionalitat de l'aplicació, detectem tres tipus d'informació a persistir: preferències d'usuari, claus i certificats digitals. Per a cadascun d'ells utilitzarem els sistemes d'emmagatzematge que per defecte ens proporciona Android.

- **Preferències d'usuari:** s'utilitzarà un fitxer de recursos xml, que residirà en la carpeta res/xml de la nostra aplicació, accedint amb la classe SharedPreferences
- **Claus:** En aquest tipus necessitem garantir la seguretat i utilitzarem el magatzem de claus de Android, accedint amb la classe KeyStore.
- **Certificats Digitals:** Utilitzarem el magatzem Android per a guardar els certificats, accedint amb la classe KeyChain

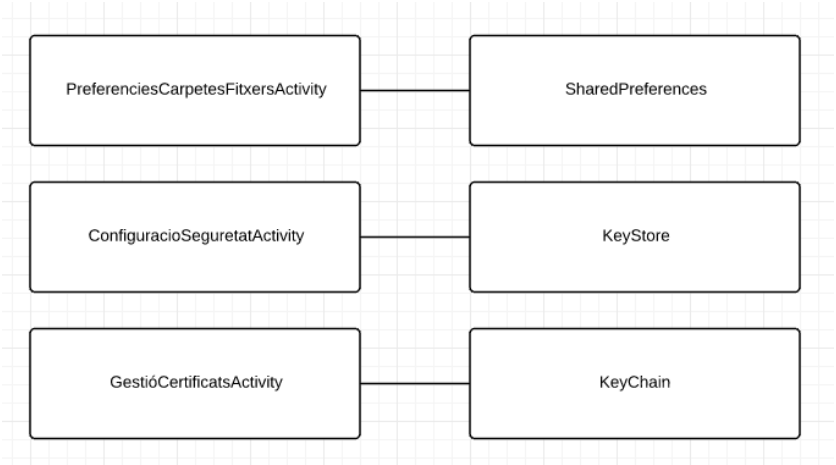


Figura 37: persistència de dades de l'aplicació

Diagrama de classes

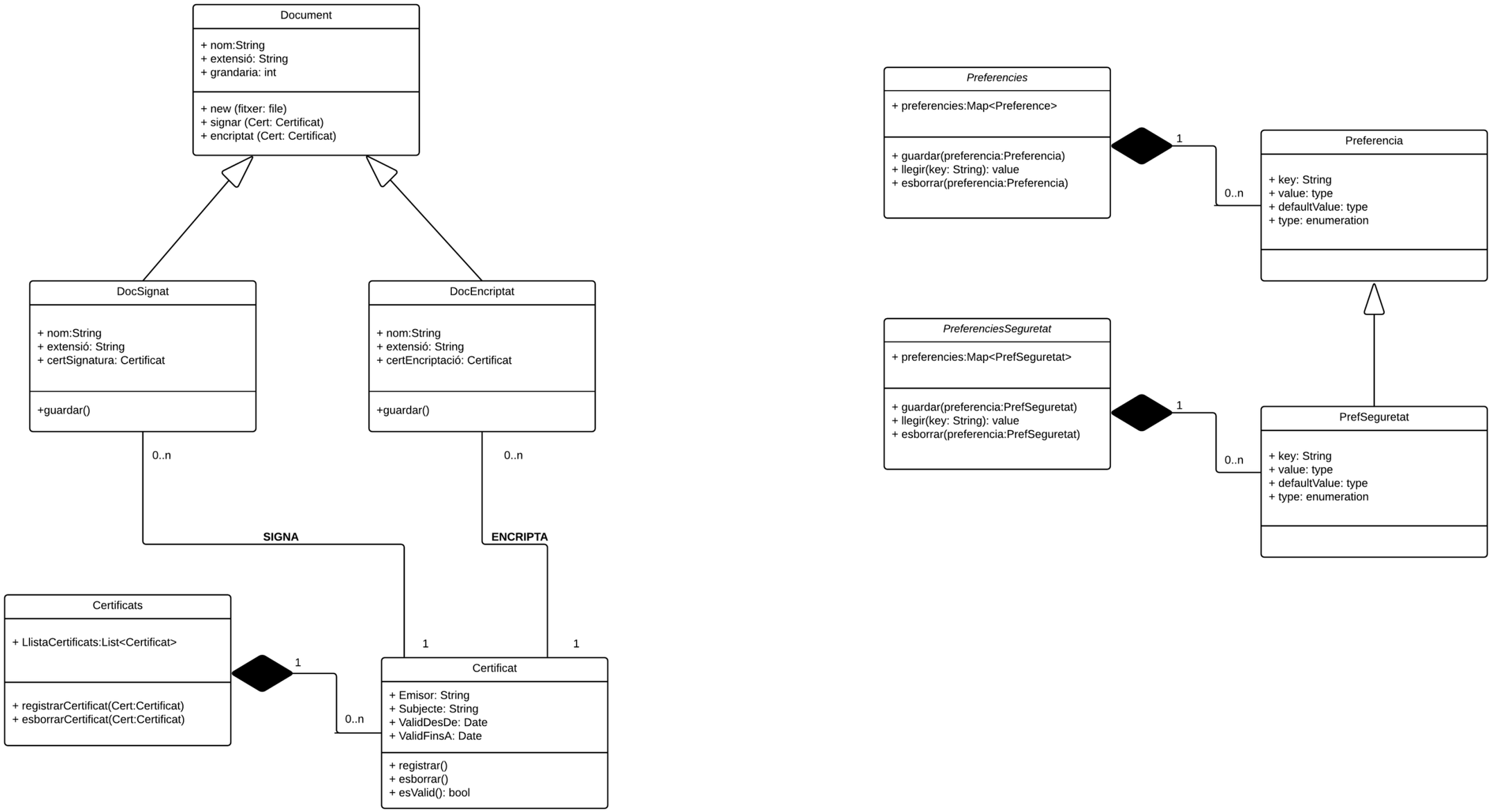


Figura 38: Diagrama de clases

Arquitectura del Sistema

L'aplicació SignaDoc no exporta informació fora del dispositiu que la conté. A continuació mostri les capes en les quals es divideix l'aplicació i la relació que té amb el sistema operatiu

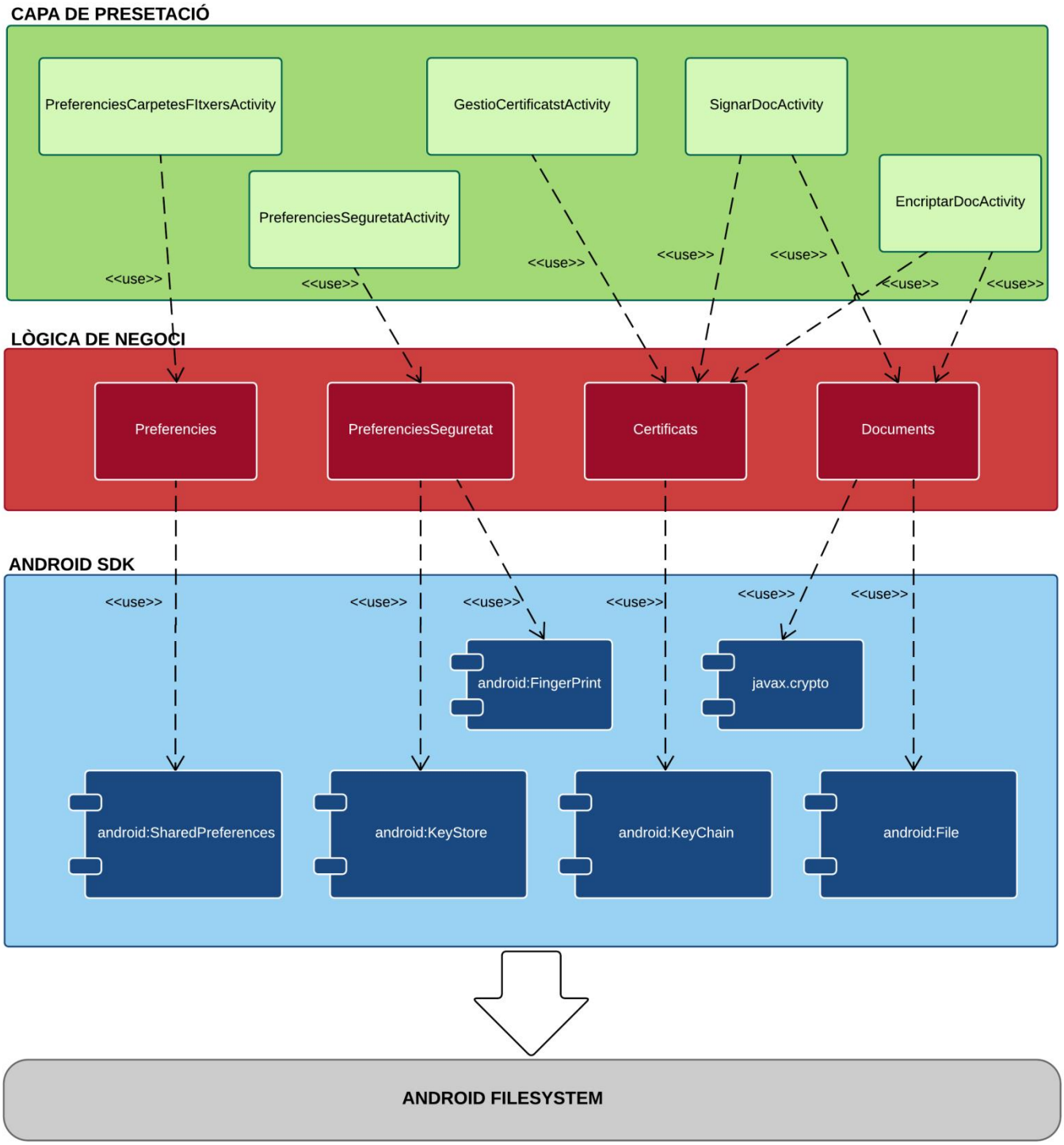


Figura 39: Arquitectura de l'aplicació

4. Implementació

Una vegada finalitzades les fases de DCU i redacció dels casos d'ús, s'ha procedit a la implementació de l'aplicació.
El desenvolupament s'ha estructurat en quatre àrees, atenent a les funcionalitats declarades en els capítols anteriors:

- Gestió de la seguretat de l'aplicació
- Gestió i ús de Certificats Digitals
- Gestió de les preferències d'usuari
- Assegurament del documents

4.1 Gestió de la seguretat de l'aplicació

Configuració del dispositiu

L'accés als magatzems de certificats en Android està protegit i el sistema no deixa accedir a ells llevat que tingues configurat el bloqueig del dispositiu, mitjançant contrasenya o patró.

A més, SignaDoc està configurada per defecte amb la restricció de sol·licitar autorització, per a signar documents o esborrar certificats, mitjançant l'escanegi de l'empremta dactilar, pel que serà necessari configurar el dispositiu amb bloqueig i registrar un empremta dactilar en el mateix.

Per a registrar una empremta, ha d'anar a l'apartat de Seguretat de la configuració del seu dispositiu i executar l'assistent per a registrar-la:

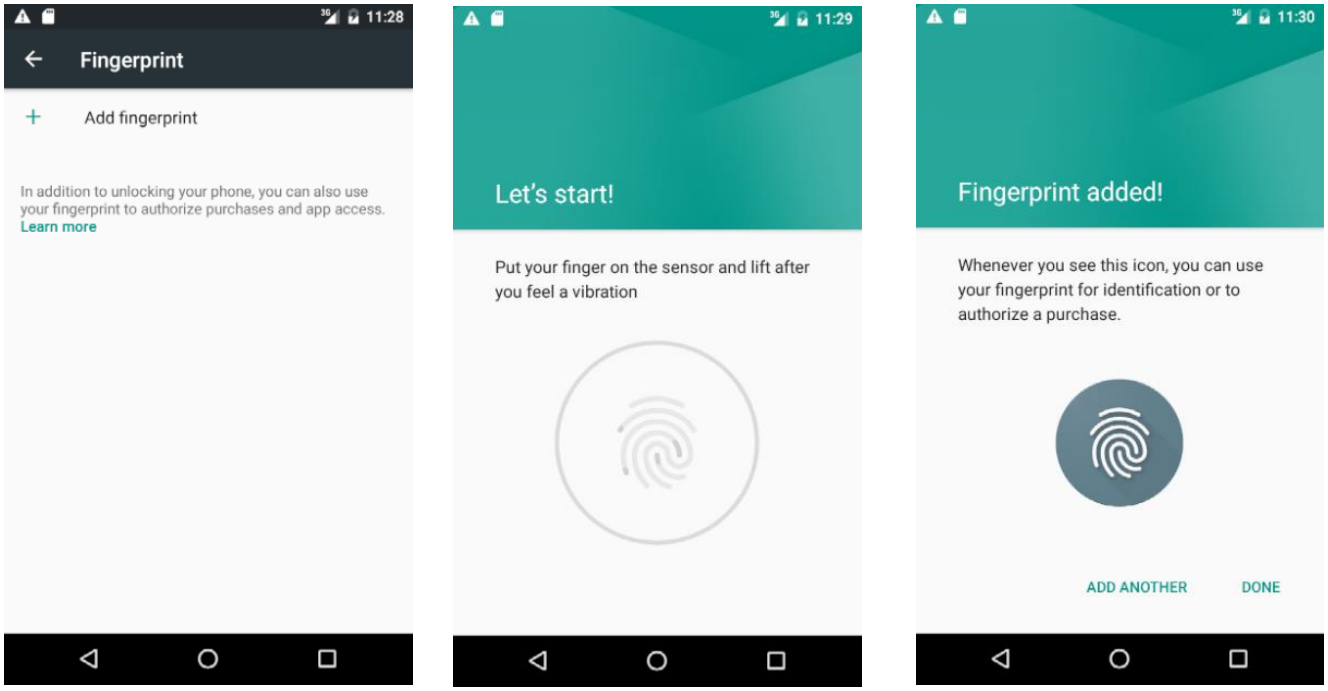


Figura 40: Registre de l'empremta dactilar al dispositiu

Configuració de l'aplicació

La configuració de la seguretat en la aplicació es fa des de la pestanya de Seguretat dins de Configuració. N´hi ha dues opcions, la de autorització per empremta, que es la recomanada i la que l'aplicació aplica per defecte i la de autorització per contrasenya, que està pensada per compatibilitat amb dispositius sense sensor.

A continuació mostri les dos opcions de configuració i com l'aplicació demana l'autorització corresponent quan es necessari:

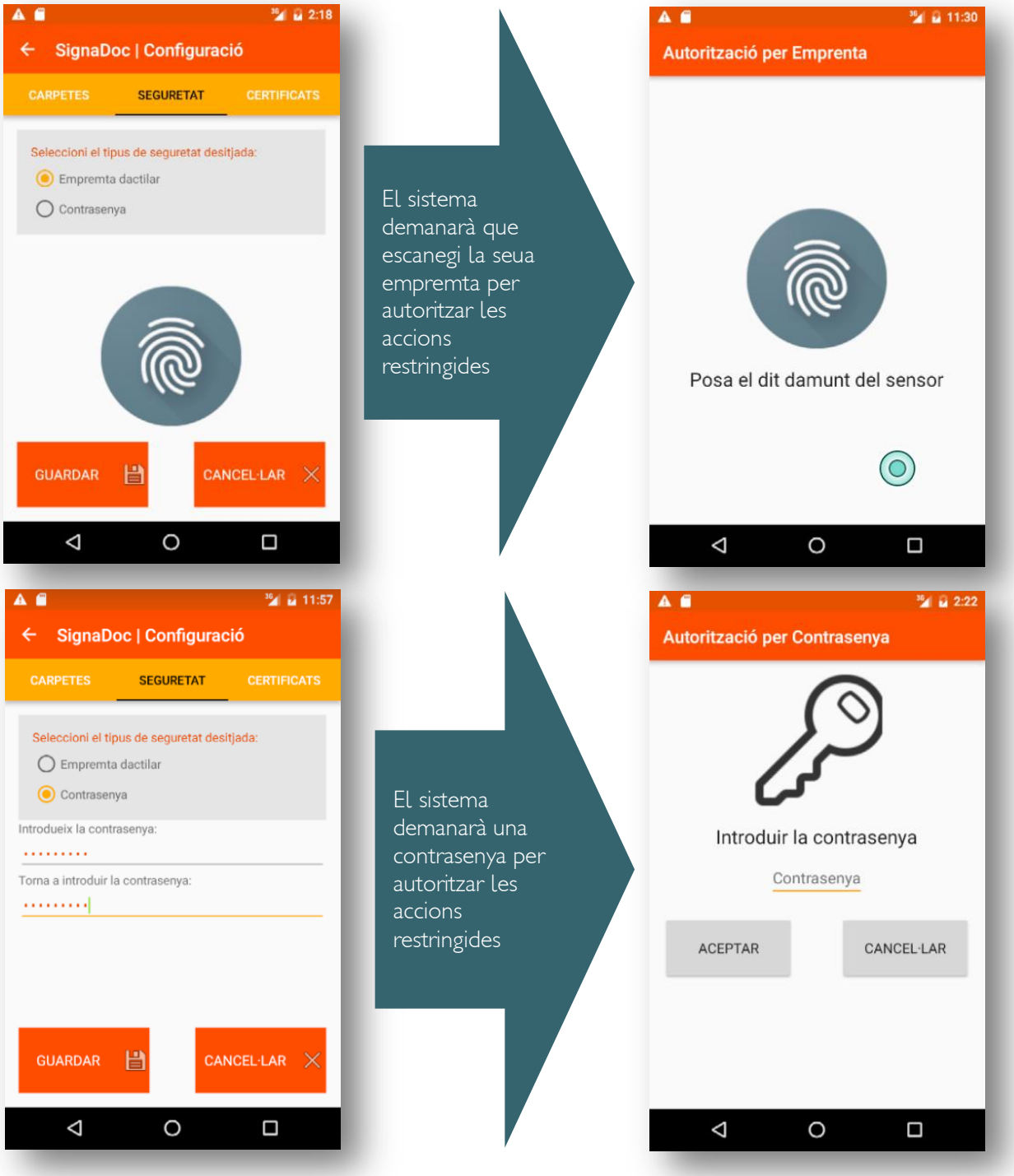


Figura 41: Configuració de la seguretat en l'aplicació

L'autenticació mitjançant empremta dactilar, ha estat introduïda en l'API d'Android en la versió 6. Els passos que cal seguir per implementar l'autenticació són (6):

1. Sol·licitud de permís d'autenticació d'empremtes digitals a l'arxiu de manifest projecte.

2. Verificar que la pantalla de bloqueig del dispositiu en el qual s'executa l'aplicació està protegida per un PIN, el patró o la contrasenya (impressions digitals només es poden registrar en dispositius en els quals s'ha obtingut la pantalla de bloqueig).

3. Assegureu-vos que almenys una empremta digital s'ha registrat en el dispositiu.

4. Crear una instància de la classe FingerprintManager.

5. Utilitzeu una instància de magatzem de claus per accedir al contenidor de claus Android. Aquesta és una àrea d'emmagatzematge utilitzat per a l'emmagatzematge segur de claus criptogràfiques en els dispositius Android.

6. Generar una clau de xifrat utilitzant la classe KeyGenerator i emmagatzemar-lo en el contenidor de claus.

7. inicialitzar una instància de la classe de xifrat usant la clau generada al pas 5.

8. Utilitzeu la instància de xifrat per crear un CryptoObject i assignar-lo a la instància FingerprintManager creat al pas 4.

9. Truqui al mètode d'autenticació de la instància FingerprintManager.

10. Implementar mètodes per manejar les devolucions de trucada desencadenades pel procés d'autenticació. Proporcionar accés al contingut protegit o funcionalitat al final d'una autenticació amb èxit.[3]

4.2 Gestió i ús de Certificats Digitals

Selecció de l'API

L'ús dels magatzems de claus en Android ha evolucionat amb cada versió del sistema operatiu. Disposem de 2 aproximacions per a l'emmagatzematge i recuperació dels certificadoes digitles en el nostre dispositiu, KeyChain y KeyStore.

Que diferencia hi ha amb el KeyChain i el KeyStore? Com triar? (6)

Segons la web Developers Android, hauríem d'utilitzar la API de KeyChain quan es volen utilitzar credencials de tot el sistema. Quan una aplicació sol·licita l'ús de qualsevol credencials a través de la API de KeyChain, els usuaris poden triar, a través d'una interfície d'usuari proporcionat pel sistema, qualsevol credencial que s'haja sigut instal·lada per qualsevol aplicació. Açò permet que diverses aplicacions utilitzen el mateix conjunt de credencials amb el consentiment de l'usuari.

Deuríem d'utilitzar el KeyStore perquè una aplicació emmagatzemi les seues pròpies credencials i que només la pròpia aplicació pugi tenir accés. Les aplicacions poden gestionar les seues credencials, al mateix temps que es proporcionen els mateixos beneficis de seguretat que la API de KeyChain proporciona per a les credencials de tot el sistema. Aquest mètode no requereix interacció amb l'usuari per a seleccionar les credencials.

[3] La classe FingerPrintActivity que utilitze en SignaDoc per a autenticar a l'usuari mitjançant la seua empremta dactilar, ha sigut adaptada de la qual ve en el tutorial de **Techotopia** (6)

KeyChain

Actualment Android ofereix KeyChain, el qual té un interfície d'alt nivell, basat en Intents i una API pública per a accedir a les claus instal·lades des de les aplicacions. La SDK API s'ocupa tant per a la gestió de certificats de confiança com de l'emmagatzematge segur de credencials. Vaig utilitzar aquesta aproximació per a la gestió dels certificats en les fases inicials del desenvolupament, ja que em va permetre dotar d'aquesta funcionalitat a la meua aplicació d'una manera ràpida.

La classe KeyChain té només 4 mètodes estàtics públics , però són suficients per a fer la majoria de les tasques relacionades amb certificats.

1.- Instal·lació de certificats digitals:

- Instal·lació del parell de claus/certificat inclosos en un arxiu PKCS#12.

```
Intent intent = KeyChain.createInstallIntent();
byte[] p12 = FileUtils.readFile(eFile.getText().toString());
intent.putExtra(KeyChain.EXTRA_PKCS12, p12);
startActivity(intent); (7)
```

- Instal·lació d'un certifado CA (Autoritat Certificadora):

```
Intent intent = KeyChain.createInstallIntent();
intent.putExtra(KeyChain.EXTRA_CERTIFICATE, CERT);
startActivity(intent); (7)
```

2.- Seleccionar un certificat: digital: és necessari cridar a KeyChain.choosePrivateKeyAlias i proporcionar una implementació de devolució de trucada que rep l'àlies seleccionat:

3.- Obtenir el clau privada d'un certificat instal·lat: utilitzem a KeyChain.getPrivateKey:

```
PrivateKey pk = KeyChain.getPrivateKey (context, alias);
```

4.-Obtenir els certificats públics associats a un certificat: utilitzem KeyChain.getCertificateChain :

```
X509Certificate[] certificates =
KeyChain.getCertificateChain (context, alias); (7)
```

Els avantatges d'utilitzar KeyChain són moltes, desenvolupament ràpid i segur de la gestió dels certificats, accés centralitzat als mateixos, encara que s'hagen introduït des de fora de la nostra app i un interfície d'usuari propi del sistema operatiu, comú a la resta de app que treballen amb certificats digitals i utilitzen aquesta classe.

Finalment s'ha desestimat aquesta aproximació, per dos motius:

1. La interfície d'usuari proporcionada s'allunya dels prototips d'alt nivell que validarem durant el DCU.
2. No ofereix la funcionalitat d'esborrar un certificat: Si bé es pot eliminar certificats de CA individuals, no hi ha manera d'esborrar els certificats d'usuari. Pot eliminar tot mitjançant l'ús de l'opció ""Esborrar credencials" en la secció d'emmagatzematge de credencials dels ajustos de seguretat.

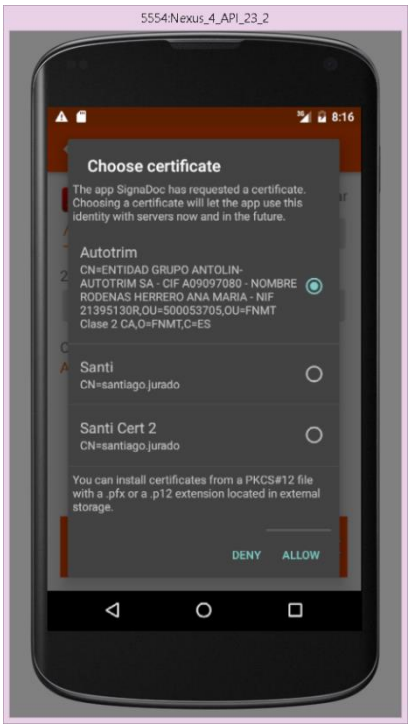


Figura 42: Selecció d'un certificat digital mitjançant el Intent proporcionat per KeyChain

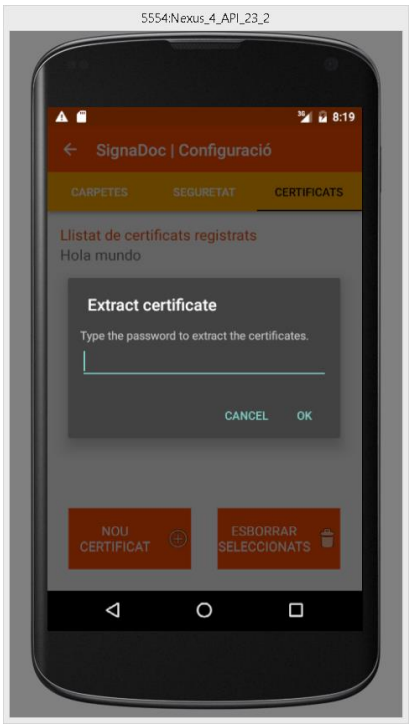


Figura 43: Intent de KeyChain per a introduir un certificat en el sistema

KeyStore

Una vegada triada la llibreria en la qual treballar, hem implementat les funcionalitats relacionades amb els certificats digitals.

Les funcionalitats són 3:

- Llistat i selecció de certificat.
- Registrar un certificat
- Esborrar un certificat

La gestió dels certificats es realitza des de la pestanya de Certificats dins de l'apartat de Configuració

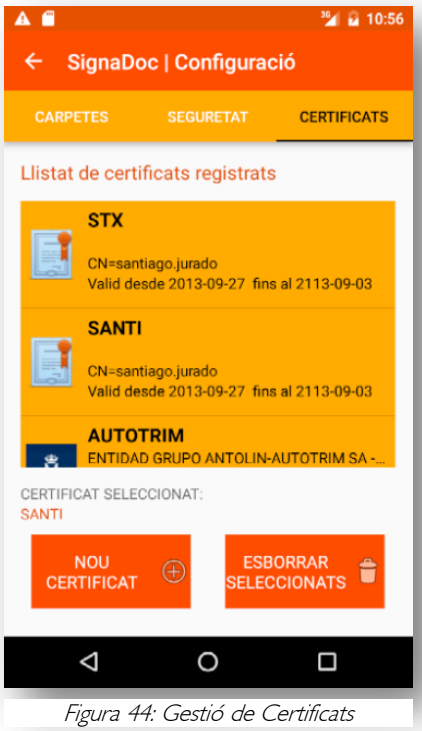


Figura 44: Gestió de Certificats

Llistat i selecció de certificat

Una vegada accedim a aquesta pestanya, ens mostrarà els certificats registrats en la nostra aplicació. Si és la primera vegada que accedim, la llista estarà buida, evidentment.

Per a llistar els certificats, s'ha utilitzat un objecte ListView, que és gestionat per un PageAdapter, la qual cosa ens permet reutilitzar aquesta vista en altres parts de l'aplicació, com en les pantalles de signatures, encriptació i des-encriptació.

Registrar un certificat

Des de la pestanya de Configuració Certificats, obrim la pantalla de registre de nou certificat, i introduïm les següents dades per a registrar-ho:

- Fitxer pfx o p12, que conté el certificat amb el parell de claus.
- La contrasenya per a exportar la clau privada
- El nom que li donarem en el nostre magatzem de certificats per a distingir-ho.

Si tot va bé, el certificat queda registrat i preparat per al seu ús

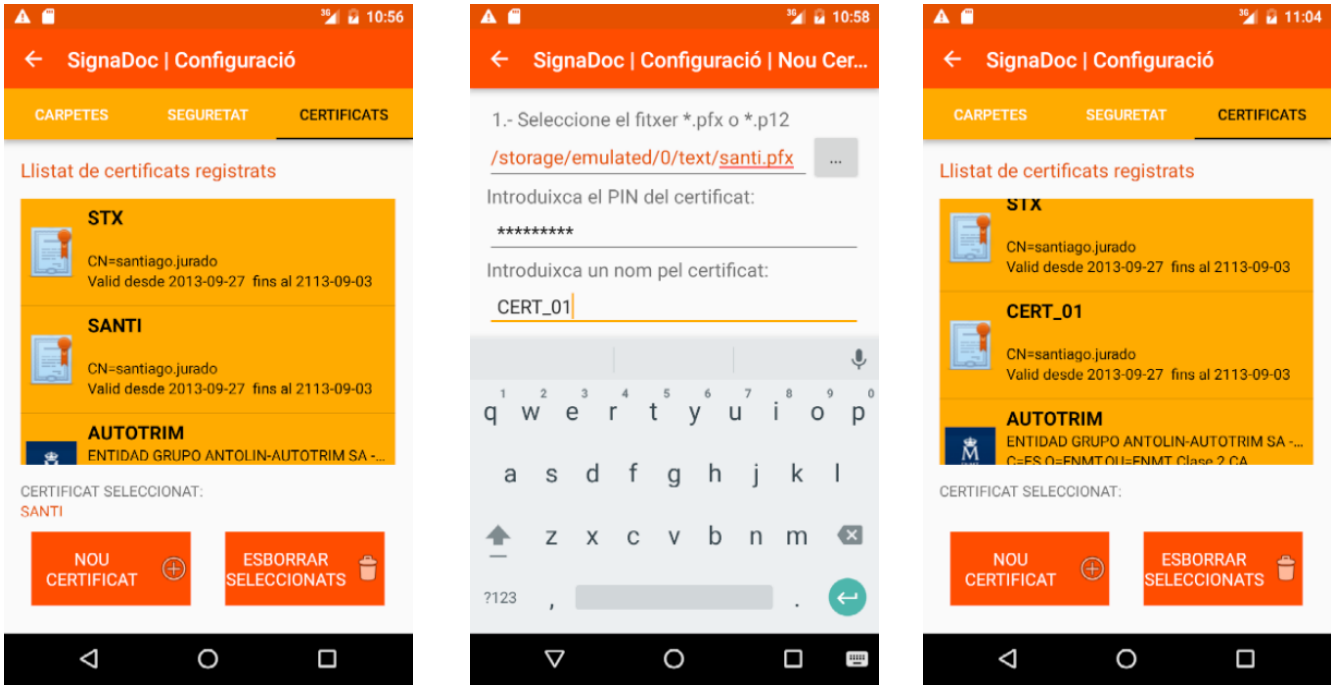


Figura 45: Registre d'un certificat

Esborrar un certificat

Des de la pestanya de Configuració Certificats, seleccionem el certificat que volem esborrar de la llista, i premem sobre el botó Esborrar.

Com és una operació crítica el sistema realitzarà una doble validació:

- Sol·licitarà l'autenticació de l'usuari
- Sol·licitarà confirmació que el certificat seleccionat és el que es vol esborrar.

Si tot va bé, el certificat quedarà eliminat del magatzem de certificats de l'aplicació.

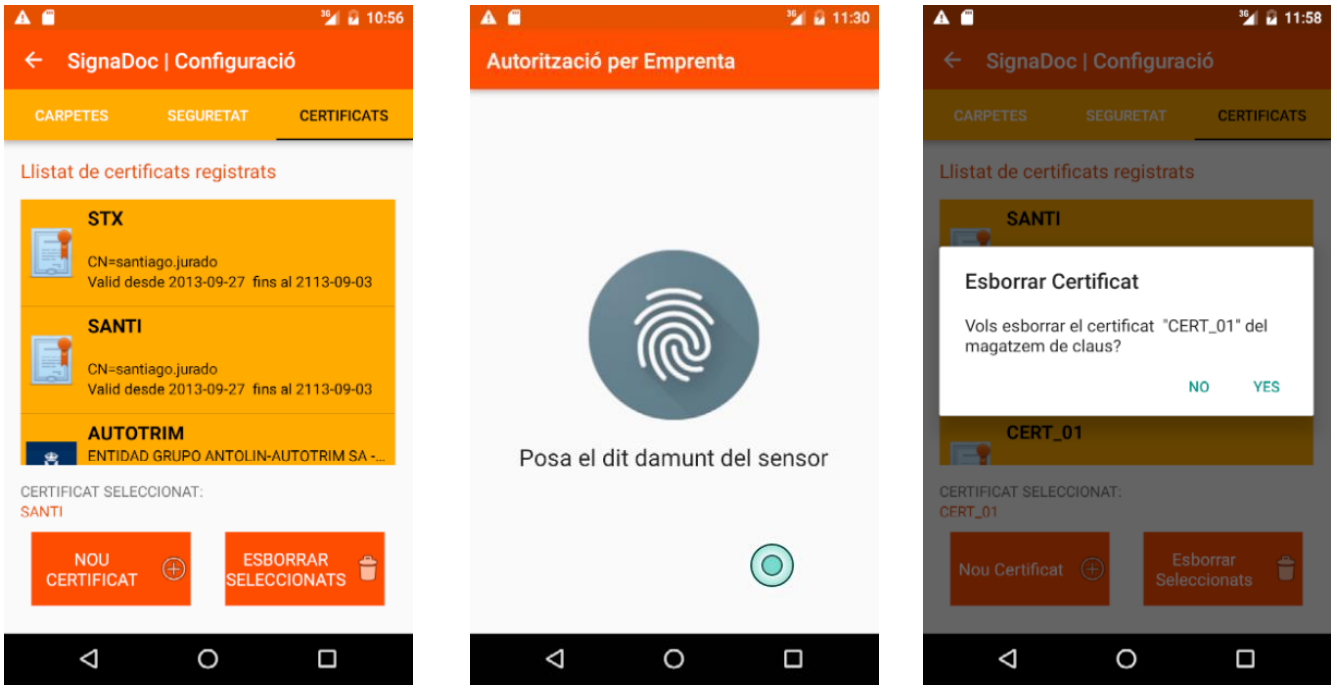


Figura 46: Esborrar un certificat

4.3 Gestió de les preferències d'usuari

En l'apartat de Configuració tenim una pestanya dedicada a les preferències de l'usuari, cridada Carpetes, on l'usuari pot indicar quals són les seues preferències, respecte del nomenat dels fitxers, dels directoris on situar els fitxers una vegada signats,..., amb que extensió vol que s'anomenen, etc.

Per a evitar errors, quan l'aplicació arranca, verifica l'existència del fitxer preferències, i si no existeix, perquè és la primera execució, construeix un amb valors per defecte.

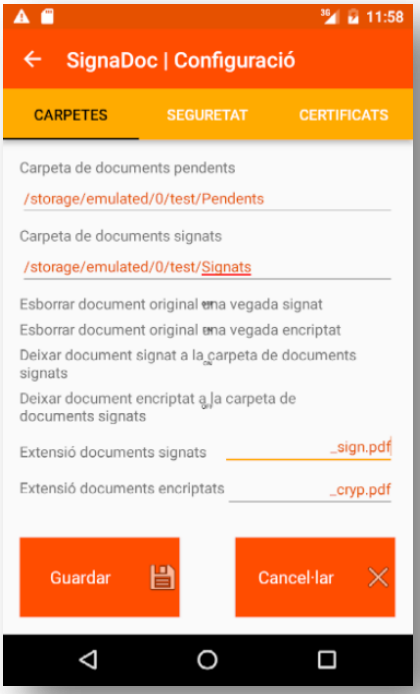


Ilustración 47: Gestió de preferències d'usuari

4.4 Assegurament de documents

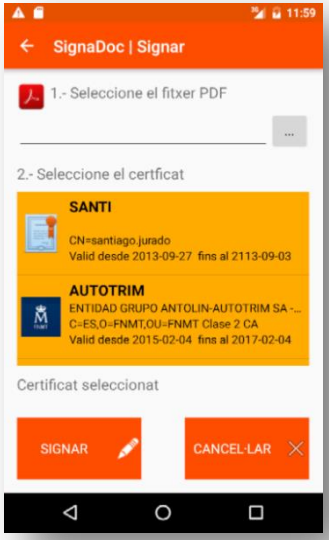
Fins ara, totes les funcionalitats que hem detallat, han servit per a tenir el nostre dispositiu preparat per a realitzar les funcions per a les quals s'ha desenvolupat aquest projecte. En aquest apartat és on ve arreplegada la funcionalitat principal de l'aplicació:

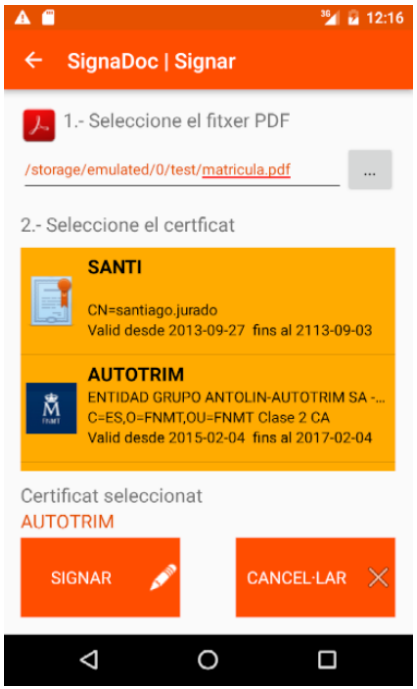
- Signatura digital d'un document PDF
- Encriptació d'un document PDF
- Des-encriptació d'un document PDF

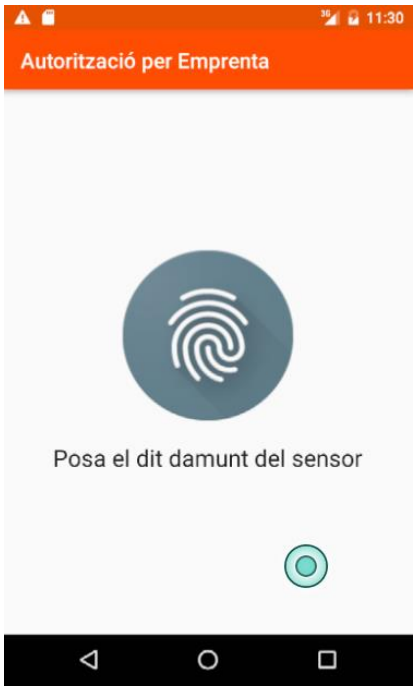
Signar un document

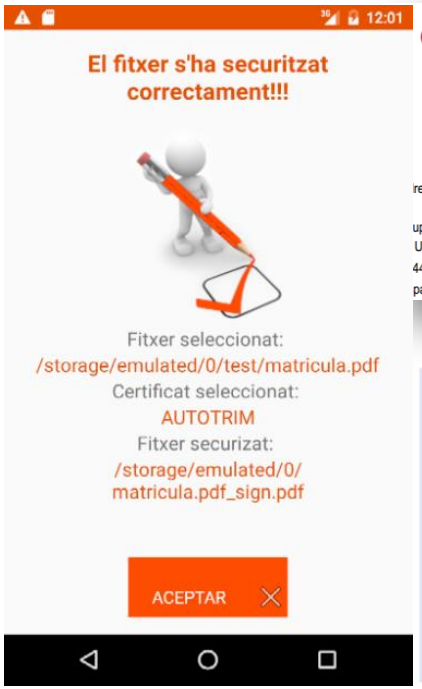
Aquesta és la funcionalitat principal de l'aplicació i que es va definir com a Objectiu Principal del Treball, en la primera part d'aquesta memòria.

El procés necessari per a dur-la a terme no ha canviat i s'ha intentat mantenir el paral·lelisme amb el prototip dissenyat en la part DCU i respectar el cas d'ús.









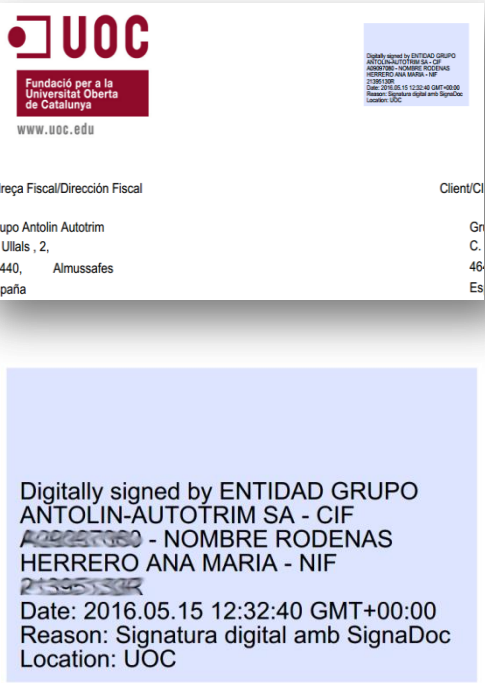


Figura 48: Signar un document

[4] Per a les proves de signatura, he utilitzat el certificat digital de la meua empresa, emès per les FNMT.

Encriptació d'un document PDF

El procés d'encriptat d'un fitxer PDF, segueix el mateix procés que el d'una signatura digital: des de la pantalla principal s'accedeix a la pantalla d'encriptació, on seleccionarem el fitxer PDF i el certificat amb el qual volem encriptar el fitxer i prèvia autenticació, el sistema crearà una còpia encriptada del fitxer, i l'anomenarà amb l'extensió triada.

Cal recalcar que en aquest context, encriptat un fitxer PDF, consisteix a protegir el seu accés mitjançant una contrasenya. El que realment fem és encriptar la contrasenya, amb la clau privada, i utilitzar-la per a protegir el document.

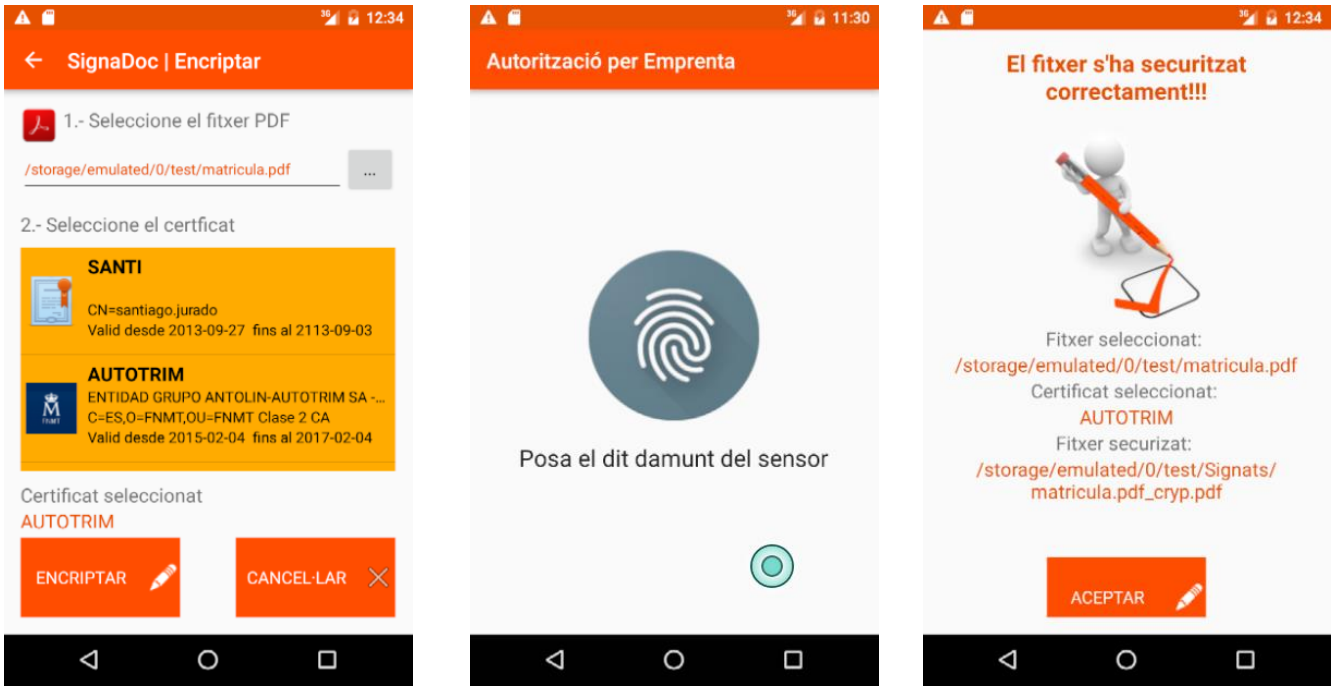


Figura 49: Encriptació d'un document PDF

una vegada protegit el document PDF, si intentem accedir, ens sol·licitarà una contrasenya. Com la mateixa ha sigut generada per la clau privada, l'únic mètode de saber-la, és revertir el procés en el següent pas.

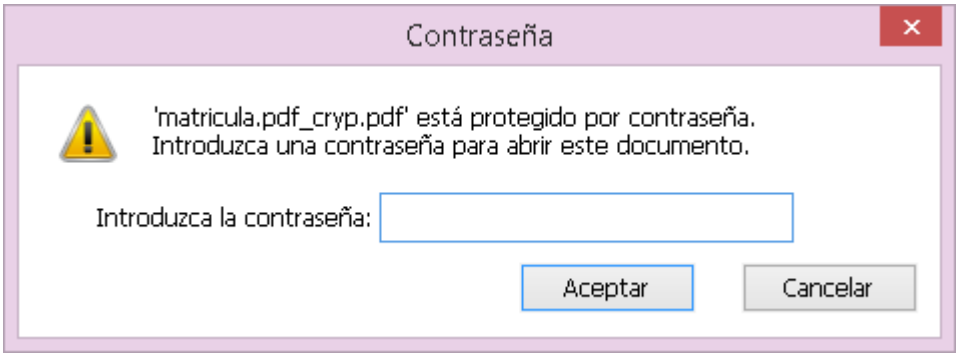


Figura50: contrasenya per accedir al document pdf

Des-encriptació d'un document PDF

El procés de des-encriptat d'un fitxer PDF, segueix el mateix procés que el d'una signatura digital i d'encriptació: des de la pantalla principal s'accedeix a la pantalla de des-encriptació, on seleccionarem el fitxer PDF encriptat i el certificat amb el qual volem des-encriptar el fitxer (que té que ser el mateix amb el qual es va encriptar) i prèvia autenticació, el sistema crearà una còpia des-encriptada del fitxer, i l'anomenarà amb l'extensió triada.

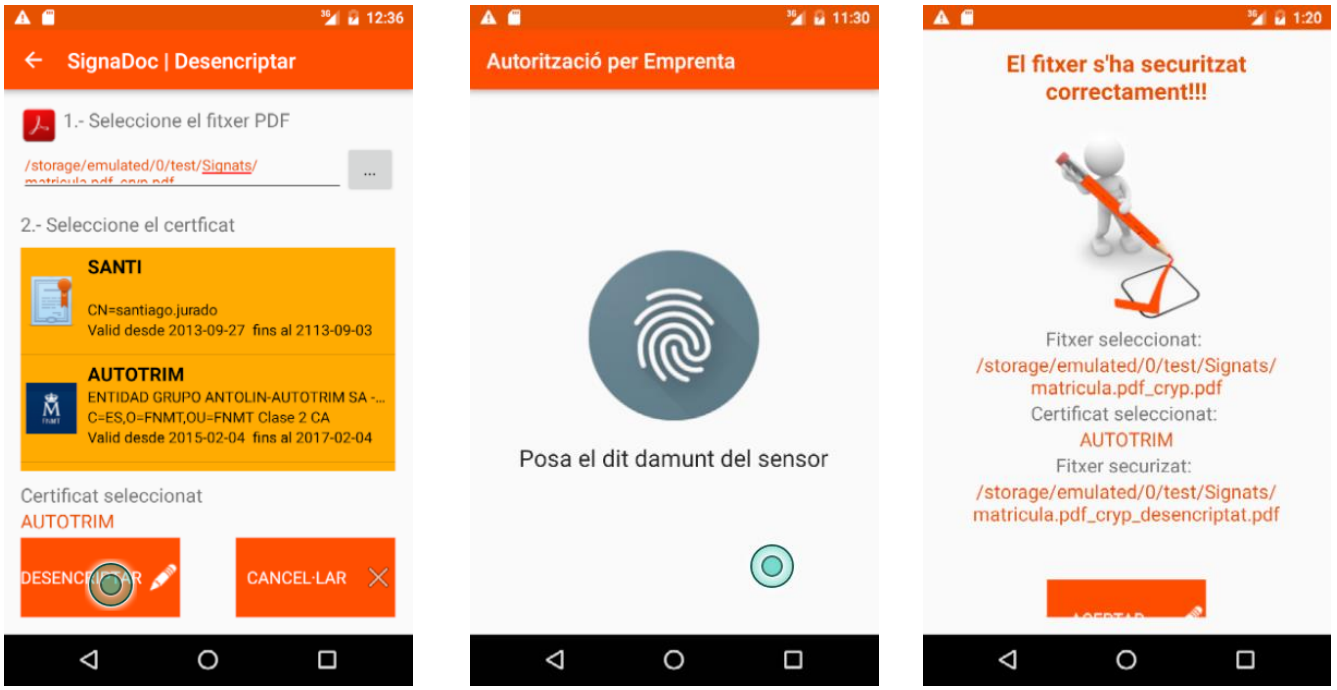


Figura 51: Des-encriptació d'un document PDF

Cal recalcar que si el fitxer seleccionat no ha segut prèviament encriptat obtindrem un error, que apareixerà amb un Toast i no es farà cap acció amb el fitxer seleccionat.
Una vegada des-encriptat el fitxer no tindrà cap restricció per accedir al seu contingut i visualitzar-ho.

Problemes amb la implementació de signatura, encriptació i des-encriptació

Per a implementar aquest apartat he utilitzat la llibreria Open Source, iText, amb llicencia AGPL, en concret la versió portada a Android, iTextG.
Les dependències d'aquesta llibreria han segut declarades en el fitxer .gradle de la aplicació:

```
compile 'com.itextpdf:itextg:5.5.9'
compile 'com.madgag:scpkix-jdk15on:1.47.0.3'
compile 'com.madgag:scprov-jdk15on:1.47.0.3'
compile 'com.madgag:sc-light-jdk15on:1.47.0.3'
```

Documentant-me en el llibre, iText in Action (9), he seguit els exemples per a signar, encriptar i desencriptar fitxers PDF.
Per a fer-ho, he creat una classe amb els 3 mètodes que necessitem:

```
public class SecureFilePdf {
    private Context context;

    public SecureFilePdf(Context context){
        this.context = context;
    }

     public void signFile(String filename, String alias, String fileSignat)
            throws GeneralSecurityException, KeyChainException, InterruptedException,
IOException, DocumentException
    {

        SignaKeyStore signaKeyStore = new SignaKeyStore(context);
        PrivateKey pk = (PrivateKey) signaKeyStore.getKey(alias);
        Certificate[] chain = signaKeyStore.getCertificateChain(alias);

        PdfReader reader = new PdfReader(filename);
        FileOutputStream os = new FileOutputStream(fileSignat);
        PdfStamper stamper = PdfStamper.createSignature(reader, os, '\0');
        PdfSignatureAppearance appearance = stamper .getSignatureAppearance();
        appearance.setReason("Signatura digital amb SignaDoc");
        appearance.setLocation("UOC");
        appearance.setVisibleSignature(new Rectangle(272, 732, 344, 780), 1,"SignaDoc");

        ExternalSignature es = new PrivateKeySignature(pk, "SHA-256","BC");
        ExternalDigest digest = new BouncyCastleDigest();
        MakeSignature.signDetached(appearance, digest, es, chain, null, null, null, 0,
MakeSignature.CryptoStandard.CMS);
    }

    public void encryptFile(String filename, String alias, String fileEncriptat)
            throws NoSuchProviderException, KeyStoreException, IOException,
CertificateException, NoSuchAlgorithmException, DocumentException,
NoSuchPaddingException, UnrecoverableEntryException, InvalidKeyException,
BadPaddingException, IllegalBlockSizeException {

        PrivateKey key = (PrivateKey) new SignaKeyStore(context).getKey(alias);
        Cipher cipher = Cipher.getInstance(key.getAlgorithm());
        cipher.init(Cipher.ENCRYPT_MODE, key);
        byte[] CLAVE = cipher.doFinal("uoc".getBytes());

        PdfReader reader = new PdfReader(filename);
        PdfStamper stamper = new PdfStamper(reader, new
FileOutputStream(fileEncriptat));
        stamper.setEncryption(CLAVE, CLAVE,
                PdfWriter.ALLOW_PRINTING, PdfWriter.ENCRYPTION_AES_128 |
PdfWriter.DO_NOT_ENCRYPT_METADATA);
        stamper.close();
        reader.close();

    }

    public void decryptFile(String filename, String alias, String fileDesencriptat)
            throws NoSuchProviderException, KeyStoreException, IOException,
CertificateException, NoSuchAlgorithmException, DocumentException,
UnrecoverableEntryException, NoSuchPaddingException, InvalidKeyException,
BadPaddingException, IllegalBlockSizeException {


        PrivateKey key = (PrivateKey) new SignaKeyStore(context).getKey(alias);
        Cipher cipher = Cipher.getInstance(key.getAlgorithm());
        cipher.init(Cipher.ENCRYPT_MODE, key);
        byte[] CLAVE = cipher.doFinal("uoc".getBytes());

        PdfReader reader = new PdfReader(filename, CLAVE);
        PdfStamper stamper = new PdfStamper(reader, new
FileOutputStream(fileDesencriptat));
        stamper.close();
        reader.close();

    }

}
```

Però en intentar executar el mètode:

```
MakeSignature.signDetached(appearance, digest, es, chain, null, null, null, 0, MakeSignature.CryptoStandard.CMS);
```

M'he trobat amb el següent error:

```
java.security.InvalidKeyException: Supplied key (android.security.keystore.AndroidKeyStoreRSAPrivateKey) is not a RSAPrivateKey instance
    at com.android.org.bouncycastle.jcajce.provider.asymmetric.rsa.DigestSignatureSpi.engineInitSign(DigestSignatureSpi.java:98)
    at java.security.Signature$SignatureImpl.engineInitSign(Signature.java:706)
    at java.security.Signature.initSign(Signature.java:357)
    at com.itextpdf.text.pdf.security.PrivateKeySignature.sign(PrivateKeySignature.java:115)
    at com.itextpdf.text.pdf.security.MakeSignature.signDetached(MakeSignature.java:151)
    at edu.uoc.santiagojurado.signadoc.crypto.SignaFile.signFile(SignaFile.java:86)
    at edu.uoc.santiagojurado.signadoc.SignarActivity$SignaFileAsync.doInBackground(SignarActivity.java:121)
    at edu.uoc.santiagojurado.signadoc.SignarActivity$SignaFileAsync.doInBackground(SignarActivity.java:111)
    at android.os.AsyncTask$2.call(AsyncTask.java:295)
    at java.util.concurrent.FutureTask.run(FutureTask.java:237)
    at android.os.AsyncTask$SerialExecutor$1.run(AsyncTask.java:234)
    at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1113)
    at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:588)
    at java.lang.Thread.run(Thread.java:818)
```

M'ocorria sempre que recuperava un certificat per mitjà de KeyChain i també quan ho recuperava a través de KeyStore d'Android. No obstant açò, quan carregava un fitxer *.pfx, directament en un KeyStore i executava el codi, funcionava correctament.
Al final, vaig optar per no utilitzar el KeyStore que proporciona Android per defecte, i crear un de propi de l'aplicació:

KeyStore d'Android:

```
private KeyStore getInstance()
        throws NoSuchProviderException, KeyStoreException, IOException,
CertificateException, NoSuchAlgorithmException {
    final KeyStore keyStore = KeyStore.getInstance("AndroidKeyStore");
    keyStore.load(null);
    return keyStore;
}
```

En crear el KeyStore de l'aplicació, he de preocupar-me de guardar el fitxer que ho conté, per la qual cosa el codi queda així:

```
private KeyStore getInstance()
    throws NoSuchProviderException, KeyStoreException, IOException,
CertificateException, NoSuchAlgorithmException {

    KeyStore keyStore = KeyStore.getInstance("pkcs12", "BC");
    if (!FileUtils.isFilePresent(FILENAME_KEYSTORE, context)) {
        FileOutputStream fOut = context.openFileOutput(FILENAME_KEYSTORE,
Context.MODE_PRIVATE);
        keyStore.load(null, null);
        keyStore.store(fOut, PW_KEYSTORE.toCharArray());
    } else {
        FileInputStream fIn = context.openFileInput(FILENAME_KEYSTORE);
        keyStore.load(fIn, PW_KEYSTORE.toCharArray());
    }
    return keyStore;
}
```

El que encara no entenc, és com un certificat guardat i recuperat dels magatzems de claus del sistema, dona un error de clau privada, quan aqueix mateix certificat, guardat i recuperat d'un KeyStore que no és el proporcionat pel sistema, funciona correctament, amb aquest mètode.
Si algú té temps i ganes, ací queda la cosa. Jo li vaig dedicar una setmana, que no tenia, i no vaig aconseguir esbrinar el misteri.

5. Proves

S´ha definit un conjunt de proves per a garantir la qualitat de l'app i facilitat el manteniment de la mateixa.

Proves unitàries

Android Studio té integrat el framework JUnit i es el que s'ha utilitzat per a fer le proves unitàries. També s´han afegit les llibreries de Mockito y Powermock. Mockito es un framework que serveix per a simular objectes externs a la classe que s'està provant. Té una limitació i es que no pot simular classes estàtiques o finals, per la qual cosa he instal·lat també el framework de proves Powermock, que sí es capaç de fer-ho.
Les dependències del projecte per a proves unitàries son les següents:

```
testCompile 'junit:junit:4.12'
testCompile 'org.mockito:mockito-core:1.10.19'
testCompile 'org.powermock:powermock-api-mockito:1.5.1'
testCompile 'org.powermock:powermock-modules:1.6.5'
testCompile "org.powermock:powermock-module-junit4:1.6.4"
```

Classe FileUtilsTest, que utilitza el framework JUnit:

```
public class FileUtilsTest {
    @Rule
    public TemporaryFolder temporaryFolder = new TemporaryFolder();
    @Rule
    public ExpectedException thrown = ExpectedException.none();

    private final String filename = "/dir1/dir2/dir3/test.pdf";


    @Test
    public void testWriteAndReadFile() throws Exception {
        File output = temporaryFolder.newFile("output.txt");
        String filename = output.getAbsolutePath();
        String test = "En un lugar de la Mancha ....";

        FileUtils.writeFile(test.getBytes(), filename);
        assertTrue(output.exists());
        byte[]resultado = FileUtils.readFile(filename);
        assertEquals(new String(resultado), test);
    }

    @Test
    public void testWriteThrowsException() throws Exception {
        String test = "En un lugar de la Mancha ....";
        thrown.expect(IOException.class);
        FileUtils.writeFile(test.getBytes(), filename);
    }

    @Test
    public void testExtractFilename() throws Exception {
        assertEquals(FileUtils.extractFilename(filename), "test.pdf");
    }

    @Test
    public void testExtractDirectoryname() throws Exception {
        assertEquals("/dir1/dir2/dir3", FileUtils.extractDirectoryname(filename));
    }

    @Test
    public void testExtractFilenameWithoutExt() throws Exception {
        assertEquals(FileUtils.extractFilenameWithoutExt(filename), "test");
    }

    @Test
    public void testGetExtension() throws Exception {
        assertEquals(FileUtils.getExtension(filename), "pdf");
    }
```

```
    @Test
    public void isFilePresent() throws Exception{
        File output = temporaryFolder.newFile("output.txt");
        String filename1 = output.getAbsolutePath();
        assertTrue(output.exists());
    }
}
```

Classe que utilitza el framework PowerMock

```
@RunWith(PowerMockRunner.class)
@PrepareForTest({KeyStore.class, SignaKeyStore.class})

public class SignaKeyStoreTest {
    private static final String FAKE_FILENAME_KEYSTORE = "fake.keystore";
    private static final String FAKE_PW_KEYSTORE = "fakePW";
    private static final String fileNamePfx = "filename.pfx";
    private static final String pingPfx = "ping";
    private static final String alias = "alias";

    @Rule
    public TemporaryFolder temporaryFolder = new TemporaryFolder();

    @Mock
    Context mMockContext;

    @Test
    public void testCreateSignaKeyStore() throws Exception{
        PowerMockito.mockStatic(KeyStore.class);
        KeyStore keyStoreMock = PowerMockito.mock(KeyStore.class);
        PowerMockito.when(KeyStore.getInstance("PKCS12",
"BC")).thenReturn(keyStoreMock);
        SignaKeyStore signaKeyStore = new SignaKeyStore(mMockContext,keyStoreMock);
        Assert.assertNotNull(signaKeyStore);
    }
```

6. Conclusions

En la realització de l'aquest projecte, vull destacar que he aconseguit respectar totes les dates i lliuraments compromesos en la planificació inicial al mateix temps que s'han completat totes les funcionalitats detectades en les fases d'anàlisis.

Com en tot projecte d'àmbit acadèmic, un dels objectius és utilitzar alguna característica nova, bé com a conseqüència del propi procés de recerca associat a aquest tipus de projectes, bé com la utilització de noves característiques oferires per les noves versions del sistema operatiu. En el meu cas he optat per utilitzar el nou API FingerPrint, que va ser alliberat en l'última versió de Android, la versió 6.

Incloure l'ús de nous API,s en un projecte, quan el desenvolupador és novençà en la tecnologia, com és el meu cas (aquesta ha sigut la meua primera app Android amb més de dues pantalles) és una mica arriscat. Cal dir respecte de Android, que no deixa de ser un risc calculat, doncs el suport que ofereix als seus desenvolupadors és impressionant, així com la filosofia de compartir coneixements que impera en la seua comunitat. Gràcies a aquest tipus d'ajuda, és possible desenvolupar aplicacions Android amb funcionalitats avançades, amb terminis molt ajustats, com solen ser els associats a la part d'implementació en els projectes de finalització de Màster, i aconseguir un resultat, que si be no pot considerar-se un producte que pot ser posat en producció, si que pot considerar-se un producte Beta, que pot ser posat a la disposició dels Beta Tester amb l'objectiu d'aconseguir un producte d'abast públic.

¿Que milloraria o afegiria a l'aplicació?

Encara que en línies generals estic molt satisfet amb l'aplicació, n´hi ha tres punts que consideri que millorarien molt la funcionalitat de l'aplicació

1. Afegiria una opció per a que l'usuari triara el lloc on apareix la signatura dins del document.
2. Afegiria altres formats de signatura:
    a. XAdES
    b. OOXML (MS Office)
    c. ODF (Open Office))
3. Afegiria l'opció de multi-signatura: en entorns professionals es molt comú que un document siga signat per més d'una persona.

Agraïments

Vull agrair a la meua família la infinita paciència que han tingut, escoltant-me parlar a tothora de certificats digitals i fent com si els interessés el tema i al seu suport donant-me ànims quan les coses no eixien com jo esperava i els terminis s'esgotaven.

7. Bibliografia

1. **FNMT.** Fábrica Nacional de Moneda y Timbre. *FNMT.* [En línia] [Data: 27 / 02 / 2016.] https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-con-android.
2. **PAE.** PAE . *Portal Administración electrónica.* [En línia] [Data: 26 / 02 / 2016.] http://firmaelectronica.gob.es/Home/Empresas/Formatos-Firma.html.
3. **RANDSTAD.** RANDSTAD. *http://www.randstad.es/.* [En línia] 17 / 06 / 2014. [Data: 27 / 02 / 2016.] http://www.randstad.es/nosotros/sala-prensa/randstad-16-06-2014.
4. **ASTIC.** ASTIC. *Asociación Profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas.* [En línia] 06 / 08 / 2015. [Data: 02 / 03 / 2016.] http://www.astic.es/noticias/modificada-la-ley-de-firma-electronica-para-habilitar-la-firma-en-la-nube.
5. No Solo Usabilidad. [En línia] [Data: 14 / 03 / 2016.] http://www.nosolousabilidad.com/articulos/dcu.htm. ISSN 1886-8592.
6. **Techotopia.** Techotopia. [En línea] 17 de 01 de 2016. http://www.techotopia.com/index.php/An_Android_Fingerprint_Authentication_Tutorial.
7. **Google.** developer.android.com. [En línea] http://developer.android.com/intl/es/training/articles/keystore.html.
8. **Elenkov, Nikolay.** Android Explorations. [En línea] 29 de 11 de 2011. https://nelenkov.blogspot.com.es/2011/11/using-ics-keychain-api.html.
9. **Lowagie, Bruno.** *iText in Action - 2nd Edition.* Stamford : Manning Publications Co., 2011. ISBN: 9781935182610.
10. **Henry, Shawn Lawton.** *Simplemente pregunta: Integración de la accesibilidad en el diseño.* Madison, WI, USA : Lawton, 2008. Versió web: www.uiaccess.com/JustAsk/es/. ISBN 978-0-9617193-2-6.
11. **Almazán, Felipe y Camus, Juan C.** *Modelo de Test de usuario.* Chile : Guía Web 2.0, 2010.

8. Annexos

En aquest apartat, no més vaig a incloure el codi font de les 2 classes que crec son una mica més importants per a entendre aquest projecte:

SecureFilePdf: Classe que encapsula la funcionalitat d'aquest projecte (signar, encriptat i des-encriptar documents pdf).

```
package edu.uoc.santiagojurado.signadoc.crypto;

import android.content.Context;
import android.security.KeyChainException;

import com.itextpdf.text.DocumentException;
import com.itextpdf.text.Rectangle;
import com.itextpdf.text.pdf.PdfReader;
import com.itextpdf.text.pdf.PdfSignatureAppearance;
import com.itextpdf.text.pdf.PdfStamper;
import com.itextpdf.text.pdf.PdfWriter;
import com.itextpdf.text.pdf.security.BouncyCastleDigest;
import com.itextpdf.text.pdf.security.ExternalDigest;
import com.itextpdf.text.pdf.security.ExternalSignature;
import com.itextpdf.text.pdf.security.MakeSignature;
import com.itextpdf.text.pdf.security.PrivateKeySignature;

import java.io.FileOutputStream;
import java.io.IOException;
import java.security.GeneralSecurityException;
import java.security.InvalidKeyException;
import java.security.KeyStoreException;
import java.security.NoSuchAlgorithmException;
import java.security.NoSuchProviderException;
import java.security.PrivateKey;
import java.security.UnrecoverableEntryException;
import java.security.cert.Certificate;
import java.security.cert.CertificateException;

import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;

import edu.uoc.santiagojurado.signadoc.util.FileUtils;

public class SecureFilePdf {
    private Context context;

    public SecureFilePdf(Context context){
        this.context = context;
    }

     public void signFile(String filename, String alias, String fileSignat, boolean
deleteOriginalFile)
            throws GeneralSecurityException, KeyChainException, InterruptedException,
IOException, DocumentException
    {
        SignaKeyStore signaKeyStore = new SignaKeyStore(context);
        PrivateKey pk = (PrivateKey) signaKeyStore.getKey(alias);
        Certificate[] chain = signaKeyStore.getCertificateChain(alias);

        PdfReader reader = new PdfReader(filename);
        FileOutputStream os = new FileOutputStream(fileSignat);
        PdfStamper stamper = PdfStamper.createSignature(reader, os, '\0');
        PdfSignatureAppearance appearance = stamper .getSignatureAppearance();
        appearance.setReason("Signatura digital amb SignaDoc");
        appearance.setLocation("UOC");
        appearance.setVisibleSignature(new Rectangle(272, 732, 344, 780), 1,"SignaDoc");

        ExternalSignature es = new PrivateKeySignature(pk, "SHA-256","BC");
        ExternalDigest digest = new BouncyCastleDigest();
        MakeSignature.signDetached(appearance, digest, es, chain, null, null, null, 0,
MakeSignature.CryptoStandard.CMS);
```

```
        if (deleteOriginalFile){
            FileUtils.deleteFile(filename);
        }
    }

    public void encryptFile(String filename, String alias, String fileEncriptat, boolean
deleteOriginalFile)
            throws NoSuchProviderException, KeyStoreException, IOException,
CertificateException, NoSuchAlgorithmException, DocumentException,
NoSuchPaddingException, UnrecoverableEntryException, InvalidKeyException,
BadPaddingException, IllegalBlockSizeException
    {
        PrivateKey key = (PrivateKey) new SignaKeyStore(context).getKey(alias);
        Cipher cipher = Cipher.getInstance(key.getAlgorithm());
        cipher.init(Cipher.ENCRYPT_MODE, key);
        byte[] CLAVE = cipher.doFinal("uoc".getBytes());

        PdfReader reader = new PdfReader(filename);
        PdfStamper stamper = new PdfStamper(reader, new
FileOutputStream(fileEncriptat));
        stamper.setEncryption(CLAVE, CLAVE,
                PdfWriter.ALLOW_PRINTING, PdfWriter.ENCRYPTION_AES_128 |
PdfWriter.DO_NOT_ENCRYPT_METADATA);
        stamper.close();
        reader.close();

        if (deleteOriginalFile){
            FileUtils.deleteFile(filename);
        }
    }

    public void decryptFile(String filename, String alias, String fileDesencriptat,
boolean deleteOriginalFile)
            throws NoSuchProviderException, KeyStoreException, IOException,
CertificateException, NoSuchAlgorithmException, DocumentException,
UnrecoverableEntryException, NoSuchPaddingException, InvalidKeyException,
BadPaddingException, IllegalBlockSizeException
    {
        PrivateKey key = (PrivateKey) new SignaKeyStore(context).getKey(alias);
        Cipher cipher = Cipher.getInstance(key.getAlgorithm());
        cipher.init(Cipher.ENCRYPT_MODE, key);
        byte[] CLAVE = cipher.doFinal("uoc".getBytes());

        PdfReader reader = new PdfReader(filename, CLAVE);
        PdfStamper stamper = new PdfStamper(reader, new
FileOutputStream(fileDesencriptat));
        stamper.close();
        reader.close();

        if (deleteOriginalFile){
            FileUtils.deleteFile(filename);
        }
    }
}
```

FingerPrintActivity: Classe que encapsula la funcionalitat d'obtenir i validar l'empremta dactilar amb la emmagatzemada en el sistema, adaptada de la que es mostra en el meravellós tutorial: *http://www.techotopia.com/index.php/An_Android_Fingerprint_Authentication_Tutorial*

```
package edu.uoc.santiagojurado.signadoc;

import android.Manifest;
import android.app.KeyguardManager;
import android.content.Context;
import android.content.Intent;
import android.content.pm.PackageManager;
import android.hardware.fingerprint.FingerprintManager;
import android.os.Bundle;
import android.os.CancellationSignal;
import android.security.keystore.KeyGenParameterSpec;
import android.security.keystore.KeyPermanentlyInvalidatedException;
import android.security.keystore.KeyProperties;
import android.support.v4.app.ActivityCompat;
import android.support.v7.app.AppCompatActivity;
import android.support.v7.widget.Toolbar;
import android.widget.Toast;

import java.io.IOException;
import java.security.InvalidAlgorithmParameterException;
import java.security.InvalidKeyException;
import java.security.KeyStore;
import java.security.KeyStoreException;
import java.security.NoSuchAlgorithmException;
import java.security.NoSuchProviderException;
import java.security.UnrecoverableKeyException;
import java.security.cert.CertificateException;

import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.SecretKey;


//http://www.techotopia.com/index.php/An_Android_Fingerprint_Authentication_Tutorial

public class FingerPrintActivity extends AppCompatActivity {

    private FingerprintManager fingerprintManager;
    private KeyguardManager keyguardManager;
    private KeyStore keyStore;
    private KeyGenerator keyGenerator;
    private Cipher cipher;
    private FingerprintManager.CryptoObject cryptoObject;
    private final String KEY_NAME = "keyFinger";


    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_finger_print);
        final Toolbar toolbar = (Toolbar) findViewById(R.id.toolbar);
        if(toolbar != null) {
            setSupportActionBar(toolbar);
            getSupportActionBar().setTitle("Autorització per Emprenta");

        }

        keyguardManager = (KeyguardManager) getSystemService(KEYGUARD_SERVICE);
        fingerprintManager = (FingerprintManager) getSystemService(FINGERPRINT_SERVICE);

        //Checking the Security Settings
        if (!keyguardManager.isKeyguardSecure()) {
            Toast.makeText(this,
                    "La pantalla de bloqueig de seguretat no està activada en
Ajustaments",
                    Toast.LENGTH_LONG).show();
            return;
        }
```

```
        if (ActivityCompat.checkSelfPermission(this,
                Manifest.permission.USE_FINGERPRINT) !=
                PackageManager.PERMISSION_GRANTED) {
            Toast.makeText(this,
                    "No tens permissos per l'ús d'Empremta dactilar",
                    Toast.LENGTH_LONG).show();
            return;
        }

        // This happens when no fingerprints are registered.
        if (!fingerprintManager.hasEnrolledFingerprints()) {
            Toast.makeText(this,
                    "Registrar almenys una empremta dactilar a Ajustaments",
                    Toast.LENGTH_LONG).show();
            return;
        }

        try {
            generateKey();
        }catch (Exception e){
            Intent i = new Intent(this, ErrorActivity.class);
            i.putExtra("MISSATGE", e.getMessage());
            startActivity(i);
            finish();
        }

        if (cipherInit()) {
            cryptoObject = new FingerprintManager.CryptoObject(cipher);
            FingerprintHandler helper = new FingerprintHandler(this);
            helper.startAuth(fingerprintManager, cryptoObject);
         }

    }


    protected void generateKey() {
        //Accessing the Android Keystore and KeyGenerator

        try {
            keyStore = KeyStore.getInstance("AndroidKeyStore");
        } catch (Exception e) {
            e.printStackTrace();
        }

        try {
            keyGenerator = KeyGenerator.getInstance(
                    KeyProperties.KEY_ALGORITHM_AES,
                    "AndroidKeyStore");
        } catch (NoSuchAlgorithmException |
                NoSuchProviderException e) {
            throw new RuntimeException(
                    "Failed to get KeyGenerator instance", e);
        }
        //Generating the Key
        try {
            keyStore.load(null);
            keyGenerator.init(new
                    KeyGenParameterSpec.Builder(KEY_NAME,
                    KeyProperties.PURPOSE_ENCRYPT |
                            KeyProperties.PURPOSE_DECRYPT)
                    .setBlockModes(KeyProperties.BLOCK_MODE_CBC)
                    .setUserAuthenticationRequired(true)
                    .setEncryptionPaddings(
                            KeyProperties.ENCRYPTION_PADDING_PKCS7)
                    .build());
            keyGenerator.generateKey();
        } catch (NoSuchAlgorithmException |
                InvalidAlgorithmParameterException
                | CertificateException | IOException e) {
            throw new RuntimeException(e);
        }
    }

    //Initializing the Cipher
    public boolean cipherInit() {
        try {
            cipher = Cipher.getInstance(
```

```
                KeyProperties.KEY_ALGORITHM_AES + "/"
                        + KeyProperties.BLOCK_MODE_CBC + "/"
                        + KeyProperties.ENCRYPTION_PADDING_PKCS7);
        } catch (NoSuchAlgorithmException |
                NoSuchPaddingException e) {
            throw new RuntimeException("Failed to get Cipher", e);
        }

        try {
            keyStore.load(null);
            SecretKey key = (SecretKey) keyStore.getKey(KEY_NAME,
                    null);
            cipher.init(Cipher.ENCRYPT_MODE, key);
            return true;
        } catch (KeyPermanentlyInvalidatedException e) {
            return false;
        } catch (KeyStoreException | CertificateException
                | UnrecoverableKeyException | IOException
                | NoSuchAlgorithmException | InvalidKeyException e) {
            throw new RuntimeException("Failed to init Cipher", e);
        }
    }

    private void returnAuthentication(int success){
        Intent data = new Intent();
        if (success==1)
            data.putExtra("authentication", true);
        else
            data.putExtra("authentication", false);
        setResult(RESULT_OK, data);
        finish();
    }


    private class FingerprintHandler extends FingerprintManager.AuthenticationCallback {
        private CancellationSignal cancellationSignal;
        private Context appContext;


        public FingerprintHandler(Context context) {
            appContext = context;
        }
        public void startAuth(FingerprintManager manager,
                              FingerprintManager.CryptoObject cryptoObject) {

            cancellationSignal = new CancellationSignal();

            if (ActivityCompat.checkSelfPermission(appContext,
                    Manifest.permission.USE_FINGERPRINT) !=
                    PackageManager.PERMISSION_GRANTED) {
                return;
            }
            manager.authenticate(cryptoObject, cancellationSignal, 0, this, null);
        }

        @Override
        public void onAuthenticationError(int errMsgId,
                                          CharSequence errString) {
            Toast.makeText(appContext,
                    "Authentication error\n" + errString,
                    Toast.LENGTH_LONG).show();
            returnAuthentication(0);
        }

        @Override
        public void onAuthenticationHelp(int helpMsgId,
                                         CharSequence helpString) {
            Toast.makeText(appContext,
                    "Authentication help\n" + helpString,
                    Toast.LENGTH_LONG).show();
            returnAuthentication(0);
        }

        @Override
        public void onAuthenticationFailed() {
            Toast.makeText(appContext,
                    "Authentication failed.",
```

```
                    Toast.LENGTH_LONG).show();
            returnAuthentication(0);
        }

        @Override
        public void onAuthenticationSucceeded(
                FingerprintManager.AuthenticationResult result) {
            Toast.makeText(appContext,
                    "Authentication succeeded.",
                    Toast.LENGTH_LONG).show();
            returnAuthentication(1);
        }
    }
}
```