UNITAT 4

SERVEIS DE FIRMA

CONTINGUTS

1 Infraestructura de clau pública PKI.....2
2 Marc normatiu de firma electrònica.....6
3 Conceptes de bàsics de firma electrònica.....6
4 Tipologia de firma electrònica.....7
5 Validació de documents signats.....8
6 Impressió de documents signats.....10
7 Serveis de firma al Govern de les Illes Balears.....11
8 ENVIAFIB, aplicació per enviar a signar documents a PORTA-FIB.....15

OBJECTIUS

1. **Conèixer els principals conceptes relacionats amb el certificat electrònic.**
2. **Tenir conceptes bàsics de firma electrònica.**
3. **Conèixer els tipus de firemes electròniques.**
4. **Sabre quins són sistemes per validar un document signat electrònicament.**
5. **Com es pot imprimir un document signat electrònicament.**
6. **Conèixer els serveis de firma de GOIB.**

1. Infraestructura de clau pública PKI

Què és un certificat electrònic?

Un certificat electrònic és l'únic mitjà que permet garantir tècnicament i legalment la identitat d'una persona a Internet. Es tracta d'un requisit indispensable perquè les institucions puguin oferir serveis segurs a través de la xarxa.

Aquest certificat consisteix en un fitxer electrònic que conté un conjunt de dades per tal d'identificar-ne el propietari.

Amb un certificat electrònic es pot intercanviar informació amb altres persones i entitats de manera segura i signar electrònicament dades per comprovar-ne la procedència i la integritat.

Figura 1: El certificat electrònic

La normativa europea **EIDAS** estableix a les condicions que tots els estats membres han de reconèixer els mitjans d'identificació electrònica de les persones físiques i jurídiques que pertanyin a un sistema d'identificació electrònica notificat d'un altre estat membre.

La normativa defineix les classes de certificats següents:

- **Certificats de firma:** vincula les dades de validació d'una firma amb una persona física i en confirma, almenys, el nom o el pseudònim.
- **Certificats de segell:** vincula les dades de validació d'un segell amb una persona jurídica i en confirma el nom.
- **Certificats d'autenticació web:** permet autenticar un lloc web i el vincula amb la persona física o jurídica a qui s'ha expedit el certificat.
- **Certificats no qualificats:** com ara SSL per establir connexions segures a Internet, certificats de component...

Què és una autoritat de certificació?

L'**Autoritat de Certificació (CA)** és una entitat de confiança, responsable d'emetre i revocar els certificats digitals utilitzats en la signatura electrònica.

A banda d'aquestes funcions bàsiques, l'**Autoritat de Certificació** pot proporcionar altres serveis com la publicació de certificats, publicació de llistes de certificats revocats, serveis de comprovació de validesa dels certificats, etc.

Figura 2: Principals autoritats de certificació

La **CA** disposa dels seus propis certificats, amb els quals firma els certificats que emet organitzats de manera jeràrquica. Una **jerarquia de certificació** consisteix en una estructura jeràrquica d'autoritats de certificació, en la qual es parteix d'una **CA Arrel** i, en cada nivell, hi ha una o més **CA** que poden signar certificats.

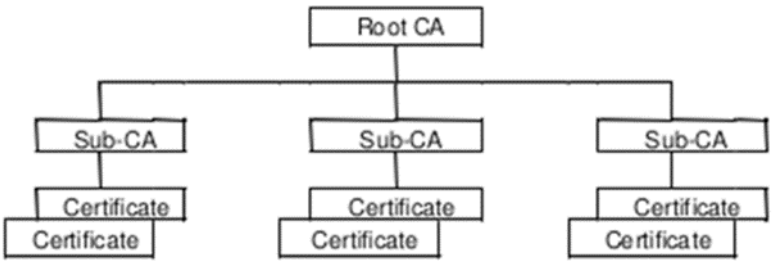

Figura 3: Jerarquia de certificats d'una CA

L'**Autoritat de Certificació (CA)**, per si mateixa o mitjançant la intervenció d'una Autoritat de Registre, verifica la identitat del sol·licitant d'un certificat abans de l'expedició.

Finalment la **CA**, per mitjà de funcions criptogràfiques, crea el certificat a partir de les dades verificades anteriorment, fet que garanteix, mitjançant una signatura electrònica, la validesa del certificat creat. Si el certificat ha estat signat electrònicament per una **CA**, l'anomenam *certificat reconegut*.

Contingut d'un certificat electrònic

Dins el fitxer del certificat podem veure la informació de la clau pública. S'obren tres pestanyes:

- **General:** es pot consultar el nom del propietari del certificat i la data de validesa.
- **Detalls:** conté la informació tècnica sobre la generació del certificat i del seu contingut.
- **Ruta de certificació:** defineix la cadena jeràrquica de certificació que dona validesa al certificat, normalment formada per un certificat arrel que firma un certificat intermedi i aquest és el que s'utilitza per firmar el nostre certificat.

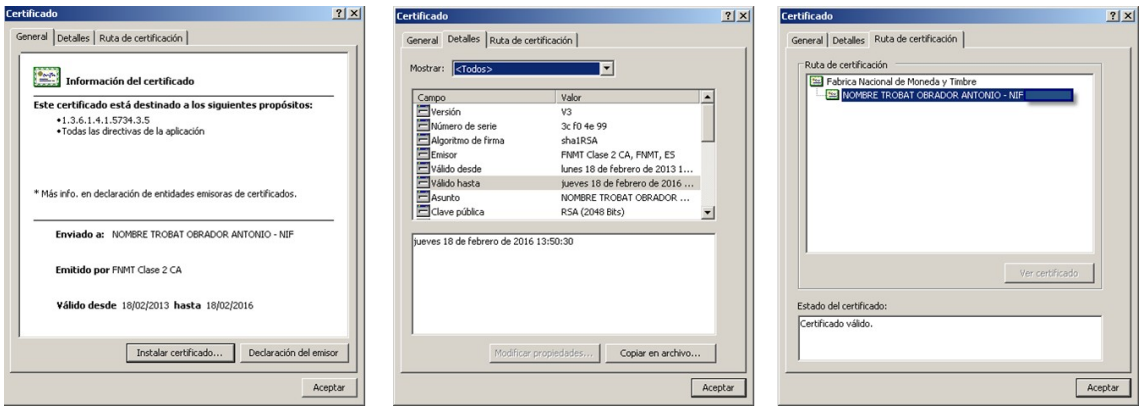

Figura 4: Contingut d'un certificat electrònic

Com es pot sol·licitar un certificat electrònic amb targeta criptogràfica al GOIB

A la pàgina *https://certificacio.caib.es* hi ha tota la informació necessària per obtenir un certificat electrònic amb targeta criptogràfica. Els passos que cal seguir són els següents:

1. Sol·licitud

Per sol·licitar un certificat electrònic de treballador públic de la CAIB heu d'iniciar un tràmit telemàtic. Cal que empleneu el formulari i hi adjunteu els documents següents:

• Còpia del DNI vigent. Si no es disposa de DNI, cal presentar un document identificatiu equivalent que incorpori una fotografia.

• Certificat que acrediti la vostra vinculació amb la CAIB. Només s'ha de presentar un dels certificats següents, en funció del cas específic.

2. Acreditació de la identitat

Una vegada finalitzat el tràmit, el personal de **l'ARCAIB (Autoritat de Registre de la CAIB)** en verificarà les dades i els documents aportats. Si tot és correcte, rebreu un correu en el qual us demanaran que us presenteu amb el DNI original (no s'admeten còpies) davant d'un **PVI (Punt de Verificació d'Identitat)**, per tal d'acreditar presencialment la vostra identitat i signar la documentació relativa a l'emissió del certificat.

3. Emissió i enviament de la targeta

Una vegada **l'ARCAIB** rebi la notificació que us heu presentat davant d'un **PVI** i heu signat els contractes, emetrà el certificat electrònic d'empleat públic en una nova targeta criptogràfica, que us enviarà per correu intern/postal a l'adreça escollida durant el tràmit inicial. Si ja disposàveu d'una targeta amb certificat electrònic, aquesta deixarà de funcionar passats 7 dies des de l'enviament o quan caduqui, si aquesta data és anterior.

2. Marc normatiu de firma electrònica

L'**article 10** de la **Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques**, regula els sistemes de firma electrònica que pot emprar l'interessat. Els sistemes de firma electrònica han d'acreditar l'autenticitat de l'expressió de voluntat i consentiment de la firma, així com la integritat i la inalterabilitat del document. Aquests sistemes de firma són:

- Sistemes de firma electrònica reconeguda o qualificada i avançada basats en certificats electrònics reconeguts o qualificats.
- Sistemes de segell electrònic reconeguts o qualificats i de segell electrònic avançat basats en certificats electrònics reconeguts o qualificats.
- Qualsevol altre sistema que es consideri vàlid.

L'**article 43** de la **Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic**, regula la firma electrònica del personal de les administracions públiques i diu que:

- Els documents electrònics s'han de signar amb una firma electrònica basada en certificats.
- La firma electrònica pot identificar el titular del lloc de treball i càrrec, així com l'Administració per a la qual fa feina. Aquest fet dona lloc a la creació de certificats electrònics de treballador públic.
- Per raons de seguretat, els sistemes de firma es poden referir només a la identificació professional de l'empleat públic. Aquest fet dona lloc a la creació de certificats de treballador públic amb pseudònim.

3. Conceptes bàsics de firma electrònica

Una firma electrònica és un conjunt de dades electròniques que acompanyen o estan associades a un document electrònic i que:

- **N'identifiquen el firmant.**
- **Asseguren la integritat** del document firmat.
- Garanteixen el **no repudi** en l'origen (qui ha firmat el document no pot negar l'autoria de la signatura).

Per firmar un document cal disposar d'un certificat digital o DNI electrònic, ja que contenen unes **claus criptogràfiques (pública i privada)** que són els elements necessaris per firmar.

Aquestes claus són complementàries, de manera que el que es xifra amb la **clau privada** només pot ser desxifrat amb la **clau pública**. El missatge desxifrat amb una **clau pública** només s'ha pogut xifrar mitjançant la clau privada, que ens permet saber qui és l'emissor del missatge.

La **clau privada** s'emmagatzema a una targeta criptogràfica protegida per un **PIN**. La clau pública s'emmagatzema al certificat electrònic del signant.

4. Tipologia de firma electrònica

Segons la normativa, es distingeixen les classes de signatura electrònica següents:

- **Signatura electrònica avançada:** és la signatura electrònica que permet identificar el signant i detectar canvis posteriors sobre les dades signades. Està vinculada al signant de manera única i a les dades originals i s'ha creat amb mitjans que el signant té sota el seu control.
- **Signatura electrònica reconeguda o qualificada:** és la signatura electrònica avançada basada en un certificat reconegut i generat mitjançant un dispositiu segur de creació de firma. A la signatura electrònica reconeguda s'atorga l'equivalència funcional amb la signatura manuscrita respecte de les dades consignades de manera electrònica.

La firma electrònica reconeguda o qualificada és l'única que es pot considerar equivalent a la firma manuscrita.

En aquestes definicions apareixen una sèrie de conceptes que ara aclarim:

- **Certificat electrònic qualificat**: certificat electrònic emès per una autoritat certificadora que ha passat un procés d'auditoria i qualitat que li atorga la capacitat d'emetre aquesta classe de certificats.
- **Dispositiu de creació de firma**: és el dispositiu en el qual s'emmagatzemen els certificats. Pot ser el magatzem de claus del sistema operatiu de l'ordinador, un navegador, un USB, una targeta criptogràfica... El nivell de

seguretat es basa en la garantia que, una vegada generada la clau privada, no es pot extreure del dispositiu. Per això, si desam el certificat al navegador o al sistema operatiu, no es considera firma feta amb un dispositiu segur, ja que és senzill extreure'n el certificat i fer-ne còpies.

- **Dispositiu segur de creació de firma qualificat:** és aquell que, per les seves característiques, ha passat un procés de certificació que n'acredita la seguretat. Acostumen a ser targetes criptogràfiques, un USB...

La **firma electrònica reconeguda** ha de:

- Identificar el firmant.
- Verificar la integritat del document firmat.
- Garantir el no repudi en l'origen.
- Disposar de la participació d'un tercer de confiança.
- Estar basat en un certificat electrònic reconegut.
- Estar generada per un dispositiu segur de creació de firma.

Els quatre primers punts són possibles gràcies a l'ús de claus criptogràfiques contingudes en el certificat i en l'existència d'**autoritats de certificació**. A més, ha d'estar basada en un certificat reconegut.

El dispositiu segur ha de garantir que les claus siguin úniques, que la clau privada no es pugui deduir de la pública i viceversa, que el signant pugui protegir de manera fiable les claus, que no s'alteri el contingut del document original i que el signant pugui veure què signarà.

La firma electrònica reconeguda i qualificada és la que es crea mitjançant un dispositiu qualificat de creació de signatures electròniques i que es basa en un certificat qualificat de signatura electrònica.

5. Validació de documents signats

Hi ha diversos mecanismes per **validar un document firmat electrònicament**. En el cas d'un document amb la **firma incrustada**, com és el cas dels PDF, el visor de PDF incorpora una eina que permet validar la firma.

La capacitat de validar d'aquesta eina varia, perquè depèn de la versió del visor de PDF que hi ha instal·lada a l'ordinador. A més, només valida la integritat del document i si el certificat està en vigor o no, no valida si el certificat està revocat.

Figura 5: Exemple de validació d'una firma dins un PDF

Per això és més recomanable utilitzar un servei qualificat per validar la firma. Per exemple, ens podem adreçar al servei **VALIDE** de validació de certificats i firma electrònica, que proporciona una validació completa de la firma.

https://valide.redsara.es

Figura 6: Plana web de Valide

6. Impressió de documents signats

La impressió d'un document firmat per una administració ha de proporcionar alguna manera per validar que el document original que té l'Administració és el mateix que el document imprès.

Per això, el procés d'impressió del document signat es reflectirà en el document en paper, a més del contingut del document:

- **Codi segur de verificació (CSV)**, per a la verificació posterior a la Seu Electrònica.
- **Dades de representació en paper de la firma.**

L'exemplar imprès del document electrònic constitueix el justificant de firma del document electrònic.

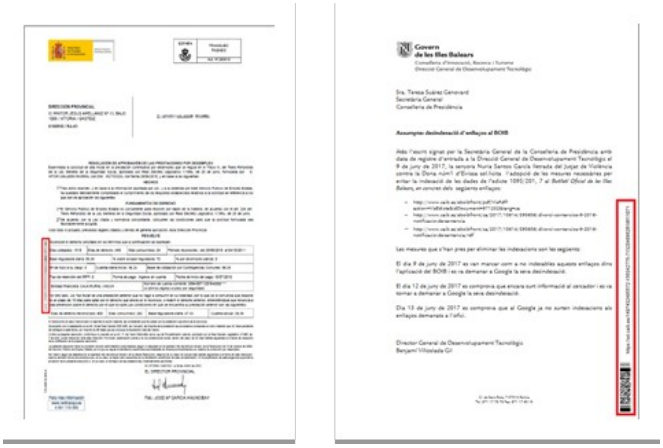

Figura 7: Exemple de documents amb CSV

El CSV ha de ser únic i estar associat a un únic document. A més, es requereix una ordre o resolució del titular de l'organisme públic, que ha de descriure el funcionament del sistema que s'utilitza per generar el CSV.

Al GOIB, l'eina per validar el document imprès és el CONCSV i està disponible a la Seu Electrònica: *https://csv.caib.es*.

Figura 8: Validador de documents de la Seu Electrònica de GOIB

Mitjançant aquesta eina, l'interessat pot introduir el codi **CSV** del document i, si hi ha un document electrònic associat, es mostrarà a l'usuari una vista del document juntament amb informació de la validesa de la firma electrònica. D'aquesta manera, l'interessat pot accedir al document, verificar-ne la integritat i contrastar-lo amb el que té en possessió.

7. Serveis de firma al Govern de les Illes Balears

Per tal de donar suport a la gestió d'expedients electrònics, el Govern de les Illes Balears disposa de diversos serveis de firma:

- **Portafirmes:** es tracta d'una aplicació informàtica que gestiona peticions de firma de documents enviats des d'altres aplicacions. Ofereix a l'usuari una safata, amb una llista de tots els documents que té pendents de signar.
- **Signatura des del navegador:** es tracta d'un servei de firma que permet signar des de la mateixa aplicació que gestiona el document electrònic que es vol signar.
- **Signatura en servidor:** és un servei de firma que permet a les aplicacions dur a terme una firma amb un certificat de segell electrònic.

PORTAFIRMES

L'aplicació de portafirmes que utilitza el **GOIB** s'anomena **PORTAFIB**. És una aplicació informàtica que gestiona peticions de firma de documents enviats des d'altres aplicacions. A més, ofereix a l'usuari una safata amb una llista de tots els documents que té pendents de signar.

S'utilitza **PORTAFIB** quan la persona que ha de firmar el document no participa directament en l'elaboració del document que s'ha de signar. El cas d'ús típic és el d'un alt càrrec (conseller, secretari, director...) que ha de signar múltiples documents i accedeix al portafirmes per signar-los, en comptes d'obrir cada plataforma de diferents eines de gestió d'expedients. D'altra banda, qualsevol usuari pot fer servir el **PORTAFIB**.

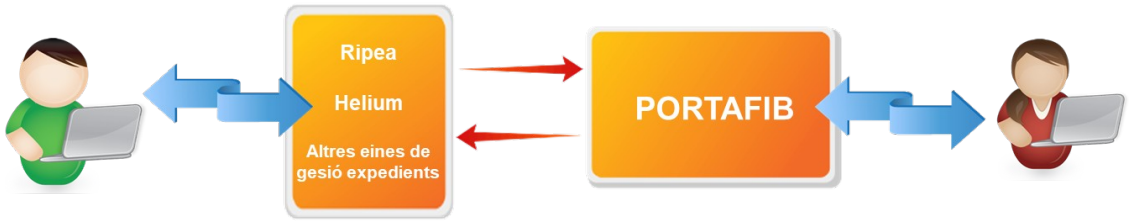

Figura 9: Funcionament de PORTAFIB

L'usuari de **PORTAFIB** accedeix a una pantalla que disposa d'una safata amb els documents pendents de firmar, una altra amb els documents firmats i, finalment, una safata amb els documents que ha rebutjat firmar.

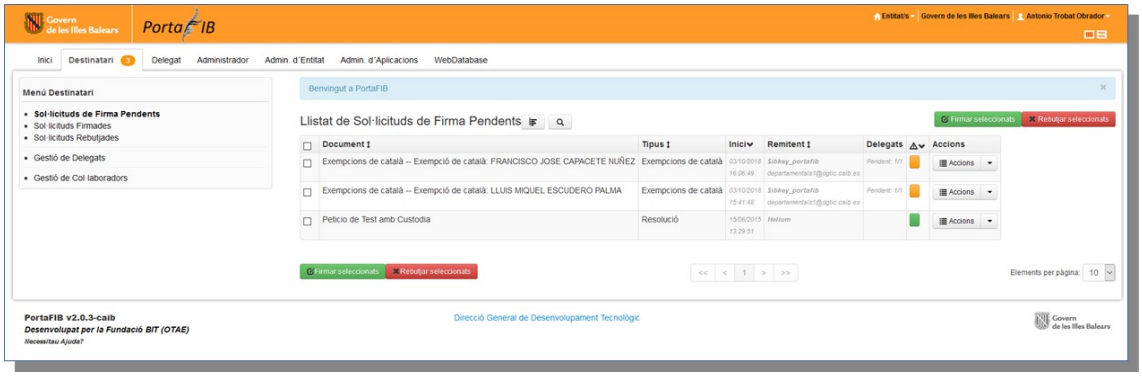

Figura 10: Pantalla de PORTAFIB

A més, aporta diverses funcionalitats importants:

- Permet configurar delegacions de firma, així com revisors que validen el document abans que passin a la safata de firma de l'usuari.
- Permet firmar múltiples documents alhora.
- Permet definir fluxos de signatura, amb el qual diverses persones firmen un mateix document. Aquests fluxos de firma poden ser en sèrie (s'estableix un ordre en els signants del document) o en paral·lel (no importa l'ordre dels signants).

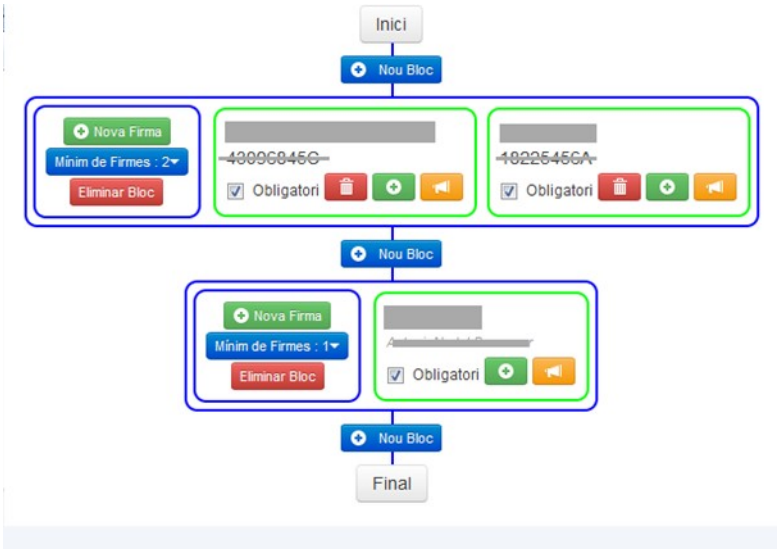

Figura 11: Asistent de creació de fluxos de firma de PORTAFIB

Signatura des del navegador

Es tracta d'un servei de firma que permet la signatura des de la mateixa aplicació que gestiona el document electrònic que es vol signar. S'utilitza quan la mateixa persona que elabora el document és qui l'ha de signar. En el moment de firmar el document, sense sortir de l'aplicació de gestió d'expedients, se cedeix el control al servei de signatura web que proporciona les eines per signar el document. Una vegada signat el control, torna a passar a l'aplicació de gestió d'expedients. Tot això és totalment transparent a l'usuari.

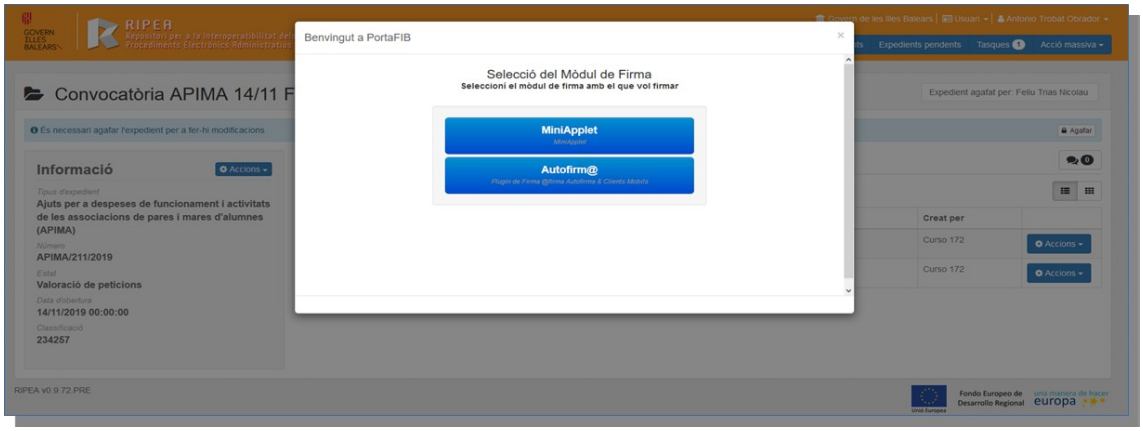

Figura 12: Servei de signatura al navegador

Signatura en servidor

És un servei de firma que permet a les aplicacions dur a terme una firma amb un certificat de segell electrònic.

En aquest cas no firma una persona amb el seu certificat, sinó que es tracta d'un segell que signa en el nom d'un òrgan. Per aquest motiu, aquest procés de firma està totalment automatitzat. L'aplicació que ha de signar els documents accedeix al servei de signatura de servidor, envia el document a signar, indica amb quin certificat de segell s'ha de signar i el servei li retorna el document ja signat.

Algunes aplicacions que utilitzen aquest servei són **DIGITALIB** que, per fer còpies autèntiques, signa els documents amb un segell de **"Còpia Autèntica del Govern de les Illes Balears"**, **REGWEB**, que signa els justificants de registre amb un segell de **"Registre Electrònic del Govern de les Illes Balears"**, o el **BOIB**, que firma els edictes publicats amb un segell de *Butlletí Oficial de les Illes Balears*.

8. ENVIAFIB, una aplicació per enviar a signar documents a PORTAFIB

ENVIAFIB és una aplicació web que permet enviar a signar documents electrònics administratius que es troben fora de l'àmbit de gestió d'un expedient administratiu. Permet a l'usuari signar documents i enviar a signar un o diversos documents a terceres persones, que poden ser tant personal intern del GOIB com usuaris externs.

ENVIAFIB facilita la gestió de peticions de signatura i la descàrrega dels documents firmats. A més, està integrada en l'Arxiu Electrònic del Govern per tal de garantir l'arxivament i la conservació dels documents signats al llarg del temps. No és necessari tenir coneixements tècnics avançats per fer servir ENVIAFIB, perquè ha estat dissenyada per ser intuïtiva i fàcil d'utilitzar per a tots els usuaris.

ENVIAFIB permet fer diverses classes d'enviaments de firma, en consonància amb el destinatari o destinataris que han de firmar el document:

- **Autofirma**: és una opció en què l'usuari signa un document des de la mateixa aplicació **d'ENVIAFIB**.
- **Enviar al director general / Enviar al secretari general:** permet enviar a signar un o diversos documents al director general de la unitat orgànica on està adscrit l'usuari **d'ENVIAFIB**, així com al secretari general de la conselleria on està ubicada la unitat orgànica on està adscrit l'usuari **d'ENVIAFIB**.
- **Firma personalitzada:** permet enviar a signar un o diversos documents, segons un flux de signatura que l'usuari defineix a través d'un assistent. Un flux de signatura permet establir un o diversos signants per a un document i definir un ordre de firmes. Aquesta opció és la ideal per a processos de signatura més complexos o per enviar a signar documents a persones que no són càrrecs com directors o secretaris generals. A través de la firma personalitzada es permet també enviar documents a usuaris externs al GOIB.
- **Els meus fluxos:** permet fer peticions de firma per mitjà de fluxos de firma que l'usuari ha creat i ha desat amb anterioritat. Amb aquesta opció podem agilitzar el procés de signatura quan l'usuari envia a signar els documents als signants.

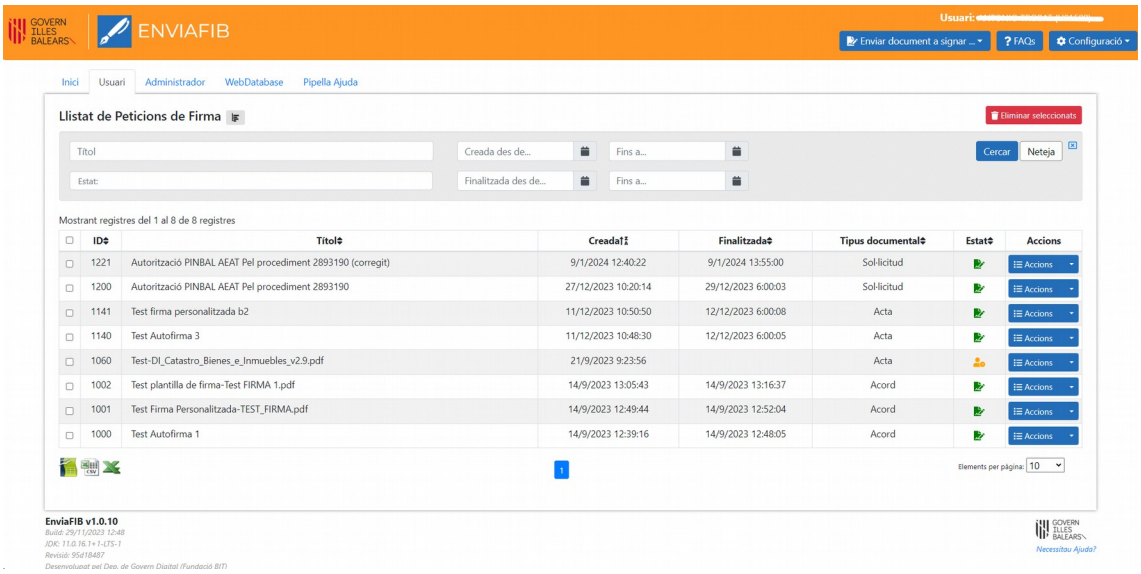

Figura 13: Pantalla principal d'ENVIAFIB.

BIBLIOGRAFIA

Reglamento UE 910/2014 del parlamento europeo y del consejo relativo a la identificación elecctrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior electrónicas en el mercado interior https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014R0910&from=IT

Jerarquia entitats de certificació https://www.securityartwork.es/2013/06/12/fundamentos-sobre-certificados-digitales-iii-cadena-de-confianza/

Llei 39/2015 del procediment administratiu comú de les administracions públiques. https://boe.es/buscar/act.php?id=BOE-A-2015-10565

Llei 40/2015 del de règim jurídic del sector públic. https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566&p=20200919&tn=2

Criptografía asimétrica https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica

Función de Hash https://es.wikipedia.org/wiki/Funci%C3%B3n_hash

Proceso de firma electrónica. https://arturomesc.files.wordpress.com/2012/10/proceso_firma_electronica.png

Validació de firma electrònica. https://valide.redsara.es/valide/validarFirma/ejecutar.html