



UNITAT 5

SERVEIS D'IDENTIFICACIÓ, SIGNATURA I REPRESENTACIÓ

CONTINGUTS

1 Serveis d'identificació.....	2
2 Serveis de signatura.....	10
3 Sistemes de representació.....	20

OBJECTIUS

1. Conèixer els serveis d'identificació que té la ciutadania: marc normatiu, característiques dels sistemes, sistema Cl@ve i component LOGINIB.
2. Aprendre què són els serveis de signatura: la infraestructura KPI, marc normatiu i conceptes bàsics de la signatura electrònica i el sistema Cl@veFirma.
3. Veure els sistemes de representació: REA, Registra Funcionaris Habilitats i Representa.



Autor/a: Servei de Sistemes d'Informació

Data d'elaboració: 29/12/2023

Aquesta obra es difon mitjançant la llicència [Creative Commons Reconeixement-NoComercial-CompartirIgual 4.0 Internacional License](https://creativecommons.org/licenses/by-nc-sa/4.0/).

1. Serveis d'identificació

1.1 Marc normatiu sobre la identificació

La Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, i la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, provoquen un canvi molt important respecte al funcionament de les administracions, ja que prioritzen el canal electrònic com a mitjà de comunicació entre ciutadans, empreses i administracions.

Internament només es permet la tramitació interna amb mitjans electrònics, la qual cosa fa que la documentació generada per les administracions hagi de ser electrònica.

Així mateix, tots els documents que entren a l'Administració ho han de fer preferentment de manera electrònica (registre electrònic, processos de digitalització...).

A l'article 9 de la Llei 39/2015 es regulen els sistemes d'identificació que tenen els interessats. A part de poder-se identificar presencialment amb el document d'identitat, s'han de definir sistemes que els permetin identificar-se de manera electrònica.

Els sistemes d'identificació electrònica necessiten un procés de registre previ com a usuari que permeti garantir la identitat d'aquest.

La Llei permet els sistemes d'identificació següents:

- Certificats electrònics reconeguts o qualificats de signatura electrònica.
- Certificats electrònics reconeguts o qualificats de segell electrònic.
- Sistemes de clau concertada (amb usuari i contrasenya).

En els apartats següents, veurem quins són aquests sistemes i com funcionen.

1.2 Descripció dels sistemes d'identificació

La normativa parla bàsicament de dos sistemes d'identificació:

- **Basats en certificats electrònics:** empren les dades que conté el certificat electrònic per identificar la persona. Durant el procés d'expedició del certificat, l'interessat s'ha d'identificar davant l'autoritat de registre que emet el certificat, per així poder validar les dades.
- **Basats en sistemes de claus concertades:** aquests sistemes es basen en la identificació mitjançant l'ús d'un sistema d'usuari i contrasenya. Durant

el procés d'alta en el sistema s'ha d'acreditar de qualque manera la identitat de l'interessat.

Segons el **Reglament comunitari de signatura electrònica (eIDAS)**, cada sistema d'identificació té un **nivell de seguretat** (baix, substancial i alt), que és requerit segons el propòsit amb què l'interessat s'ha de relacionar amb l'Administració. No és el mateix, per exemple, sol·licitar una cita per al metge que fer una sol·licitud per iniciar un procediment de voluntats anticipades.

- El **nivell de seguretat baix** fa referència a un sistema electrònic d'identificació que estableix un grau limitat de confiança en la identitat de la persona que s'identifica. Té com a objectiu reduir el risc d'ús indegut o alteració de la identitat presentada.
- El **nivell de seguretat substancial** fa referència a un sistema electrònic d'identificació que estableix un grau substancial de confiança en la identitat de la persona que s'identifica. Té com a objectiu reduir substancialment els riscos d'ús indegut o alteració de la identitat presentada.
- El **nivell de seguretat alt** fa referència a un sistema electrònic d'identificació que estableix un grau alt de confiança en la identitat de la persona que s'identifica. Té com a objectiu **evitar** l'ús indegut o l'alteració de la identitat.

El nivell de seguretat està relacionat amb la rigorositat del procés de registre que ha seguit l'interessat. Aquest serà més rigorós, si l'interessat s'ha personat davant una entitat autoritzada per fer el registre d'alta en el sistema d'identificació, que si el procés es fa només telemàticament.

1.3 Sistema d'identificació ciutadana: Cl@ve

Cl@ve és un sistema orientat a unificar i simplificar l'accés electrònic dels ciutadans als serveis públics. L'objectiu principal és que el ciutadà es pugui identificar davant l'Administració mitjançant claus concertades (usuari i contrasenya), sense haver de recordar claus diferents per accedir als diversos serveis.

Cl@ve permet utilitzar sistemes d'identificació basats en claus concertades (sistemes d'usuari i contrasenya) i certificats electrònics (DNIE inclòs).

Requereix registre previ, bé de manera presencial o telemàtica. El registre telemàtic es pot fer mitjançant certificat electrònic o dades conegudes per ambdues parts (informació tributària).

El 19 de setembre del 2014, mitjançant Acord del Consell de Ministres, es va aprovar que Cl@ve fos el sistema d'identificació, autenticació i signatura electrònica comú per a tot el sector públic estatal.

En aquest Acord es preveu la possibilitat que altres administracions públiques es puguin adherir al sistema mitjançant conveni, d'acord amb les condicions tècniques, econòmiques i organitzatives que pertoquin.

Pel que fa a les claus concertades, Cl@ve admet dues possibilitats d'ús.

- **Cl@ve ocasional (Cl@ve PIN):** sistema de contrasenya de validesa molt limitada en el temps, orientat a usuaris que accedeixen esporàdicament als serveis, que es correspon amb el sistema PIN24H de l'AEAT.
- **Cl@ve Permanent:** sistema de contrasenya de validesa duradora en el temps, però no il·limitada, orientat a usuaris habituals. Es correspon amb el sistema d'accés mitjançant usuari i contrasenya, reforçat amb claus d'un sol ús per SMS, per accedir als serveis de la seguretat social.

Per poder emprar aquestes claus concertades i els serveis de signatura al núvol, els ciutadans s'han de registrar prèviament al sistema i facilitar les dades personals necessàries.

1.4 Procés de registre a Cl@ve

Segons l'article 9.2 de la Llei 39/2015, els interessats es poden identificar electrònicament davant les administracions públiques, a través de certificats electrònics o qualsevol sistema que disposi d'un registre previ que permeti garantir la seva identitat.

Cl@ve permet registrar-se mitjançant quatre vies:

1. Per Internet a partir d'una carta d'invitació.
2. Per Internet per videotrucada.
3. Amb certificat electrònic.
4. De manera presencial.



Figura 1: Registre a Cl@ve.

Segons la via triada, es proporciona a l'interessat un nivell de registre:

- **Registre bàsic:** si tria les vies 1 i 2. Les dades de registre d'usuari les facilita el ciutadà telemàticament, utilitzant dades que coneix el ciutadà i l'Administració.

The screenshot shows the '¿Cómo puedo registrarme?' page with the first option selected: 'A través de Internet sin certificado electrónico'. Below this, it says 'Registro Nivel Básico' and explains that the process consists of two steps. The first step is to request a 'Carta de Invitación' (Invitation Card) by providing basic identification data. The second step is to complete the registration by providing the necessary data to use Cl@ve. The form for the first step is titled 'Solicitud de carta de invitación' and includes fields for 'Identificación', 'NIF', 'Primer apellido', and 'Número de cuenta bancaria'. There is also a section for 'IBAN' with a dropdown menu and a 'Enviar' button. At the bottom, there are links for '¿Qué es el código IBAN y cómo puede obtenerse?' and '¿Cómo debo comentar el Número de cuenta bancaria IBAN en este formulario?'.

Figura 2: Registre bàsic a Cl@ve.

- **Registre avançat:** si tria les vies 3 i 4. Les dades les facilita el ciutadà de manera presencial en una oficina davant un empleat públic habilitat, o de manera telemàtica amb un certificat electrònic reconegut.

1.5 Funcionament del sistema Cl@ve

• Pas 1. Accedeix al sistema

Per fer servir les teves contrasenyes de Cl@ve en un servei d'administració electrònica, únicament has de fer clic a la icona a la pantalla d'accés al servei (per exemple, seleccionant un procediment o servei de la Seu Electrònica del Govern amb tràmit telemàtic).

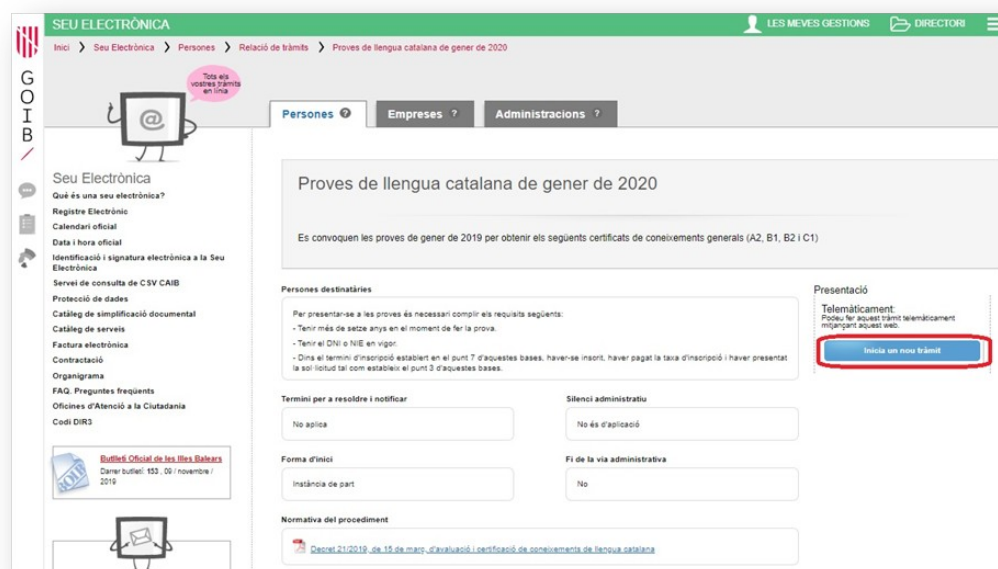


Figura 3: Iniciar un tràmit telemàtic des de la Seu Electrònica del GOIB.

• Pas 2. Selecciona el mètode d'identificació

A continuació, seràs redirigit al sistema corporatiu d'autenticació (LOGI-NIB), i si selecciones l'opció Cl@ve podràs triar el mètode d'identificació.

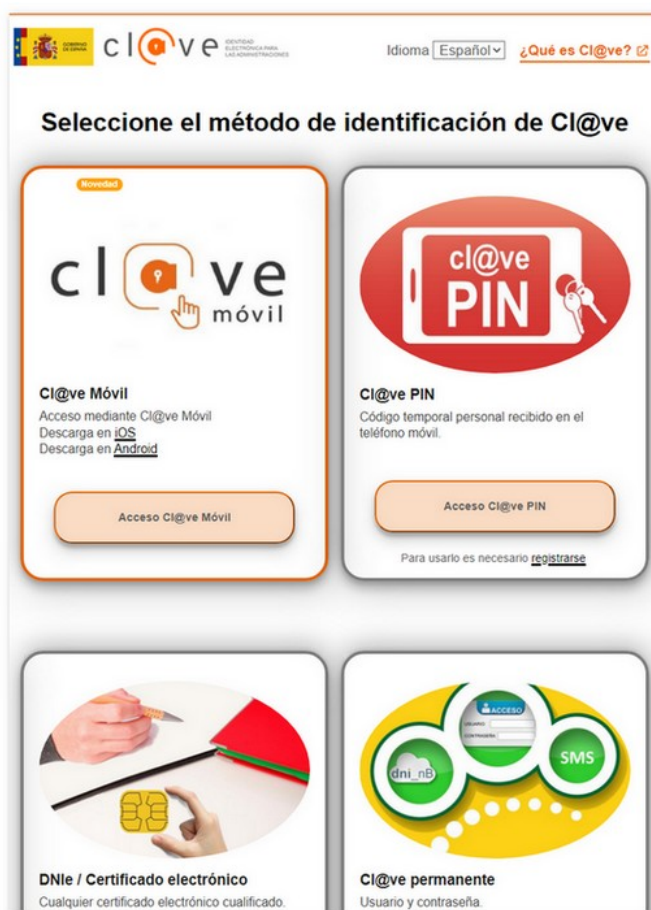


Figura 4: Els diferents mètodes d'identificació de Cl@ve.

- A la pantalla de Cl@ve trobaràs un selector que et permetrà triar un dels mètodes d'identificació disponibles per al servei en qüestió (recorda que només es permeten els mètodes que proporcionen un nivell de seguretat en l'accés igual o superior al que necessita el servei). Els mètodes d'identificació no disponibles apareixeran en tonalitats grises (desactivats). Per seleccionar el mètode d'identificació, fes clic a Accedir.

• Pas 3. Identifica't

Una vegada has triat el mètode per identificar-te, Cl@ve et redirigirà a la pantalla d'identificació. Aquesta pantalla és diferent depenent del mètode seleccionat.

En el cas d'emprar la Cl@ve ocasional, (Cl@ve PIN), apareixerà la pantalla següent:

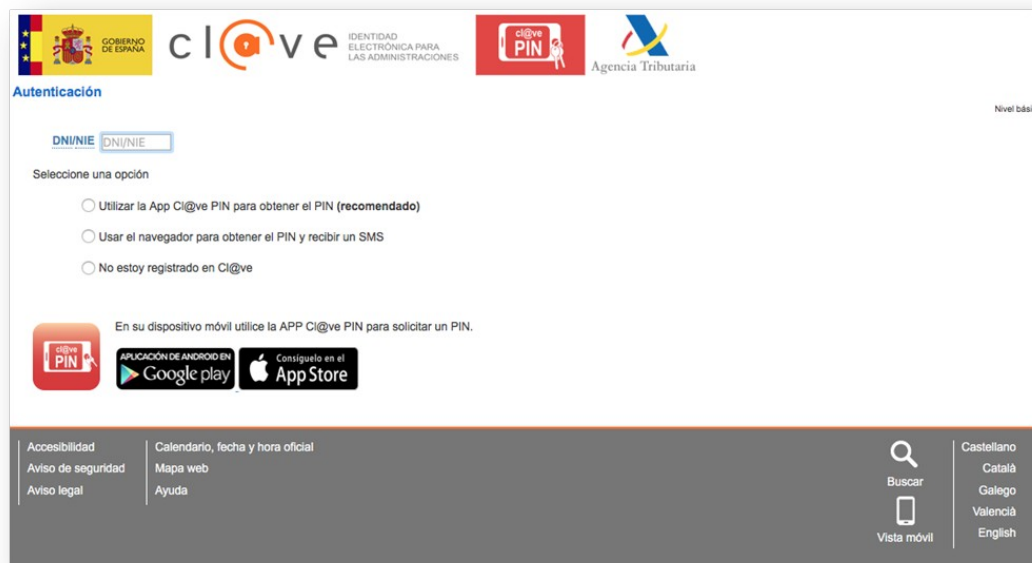


Figura 5: Identificació mitjançant Cl@ve PIN.

• Pas 4. Torna al servei d'administració electrònica

Una vegada t'hagis identificat correctament, Cl@ve et retornarà novament al servei que ha sol·licitat l'autenticació amb les teves credencials (seguint amb l'exemple, et redirigirà de nou a la Seu Electrònica i passa les credencials a l'assistent de tramitació telemàtica del Govern).

1.6 Component corporatiu d'autenticació: LOGINIB

LOGINIB és el component corporatiu d'autenticació ciutadana. Mitjançant aquesta aplicació, es proveeix als diferents sistemes del Govern d'un servei d'identificació ciutadana.

Aquest component inclou la gestió de la pàgina de login, permet l'accés anònim (pensat per accedir a serveis administratius) i la utilització de Cl@ve autenticació (pensat per a l'accés a procediments administratius).

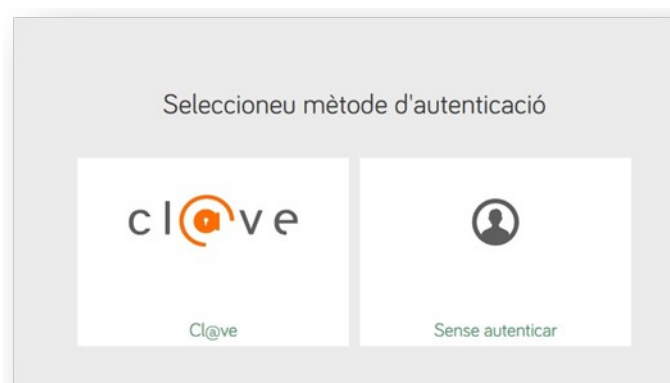


Figura 6: Component corporatiu d'autenticació: LOGINIB.

Tot seguit analitzarem amb més detall els diferents sistemes d'identificació que proporciona Cl@ve:

- Clave PIN.
- Cl@ve Permanent.
- Cl@ve Mòbil.
- Certificat Digital.

1.6.1 Cl@ve PIN

Per obtenir Cl@ve PIN des d'Internet, has de fer clic al botó «No tengo PIN».



Figura 7: Opció "No tengo PIN" de Cl@ve.

A continuació has d'emplenar el formulari (DNI i data de validesa) i pitjar el botó d'obtenir PIN. Una vegada demanat el PIN, rebràs un missatge al mòbil amb el pin.



Figura 8: Formulari per emplenar i poder rebre el missatge amb el pin.

Per obtenir el pin des del mòbil, has de suggerir un codi, pitjar el botó enviar i a través d'aquell codi l'app et donarà un pin.

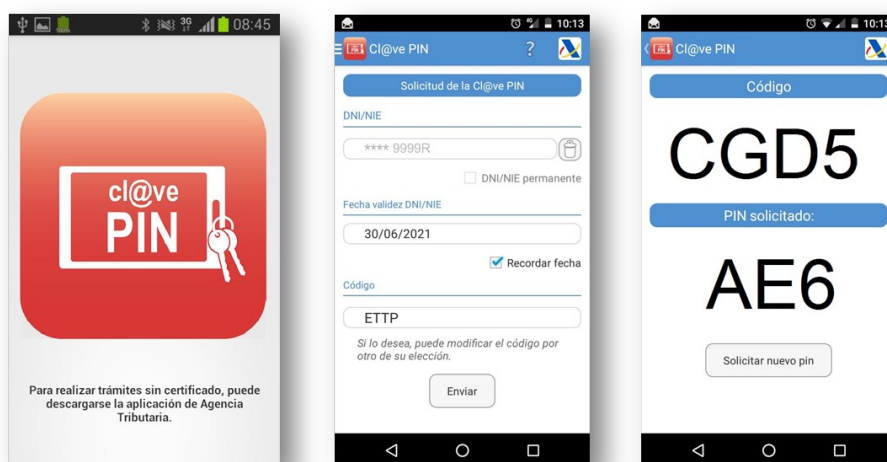


Figura 9: Obtenció del pin a partir d'un codi.

1.6.2 Cl@ve Permanent

Està pensat per a persones que necessiten accedir sovint als serveis electrònics de l'Administració. Es basa en la utilització d'un codi d'usuari, DNI o NIE i una contrasenya que s'estableix en el procés d'activació. Per accedir al procés d'activació és necessari estar registrat al sistema.



Figura 10: Cl@ve permanent.

Per als serveis d'administració electrònica que requereixin un nivell de seguretat elevat, el sistema reforça l'autenticació amb un codi d'un sol ús que s'envia prèviament per SMS al teu dispositiu mòbil.

1.6.3 Cl@ve Mòbil

Cl@ve Mòbil és el nou sistema d'accés electrònic als serveis públics que permet al ciutadà autenticar-se en el tràmit que estigui realitzant, simplement confirmant la petició d'autenticació que rep a l'aplicació mòbil Cl@ve.

És un sistema senzill, amb el qual l'usuari no ha de recordar cap contrasenya; només ha d'obrir l'aplicació de mòbil de Cl@ve (APP Cl@ve) i confirmar la petició d'autenticació que rep. Una vegada fet això, pot accedir al tràmit que vol efectuar.

1.6.4 Cl@ve amb certificat electrònic

Cl@ve també et permet identificar amb DNIE o certificat electrònic. Si selecciones aquest mètode, apareix una pantalla que canvia segons el navegador i on pots triar el certificat que vols emprar. Una vegada seleccionat, el sistema t'identifica.

2. Serveis de signatura

2.1 Infraestructura de clau pública PKI

2.1.1 Què és 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 d'Internet.

El certificat electrònic és un fitxer electrònic que conté un conjunt de dades per tal d'identificar el seu 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 integritat.



Figura 11: Propietats d'un certificat electrònic.

La normativa Europea eIDAS estableix les condicions amb què 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.

Defineix els tipus de certificats següents:

- **Certificats de signatura:** vincula les dades de validació d'una signatura amb una persona física i confirma, almenys, el nom o el pseudònim d'aquella persona.
- **Certificats de segell:** vincula les dades de validació d'un segell amb una persona jurídica i confirma el nom d'aquella persona.
- **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** (SSL per establir connexions segures a Internet, certificats de component...).

2.1.2 Què és una autoritat de certificació?

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

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

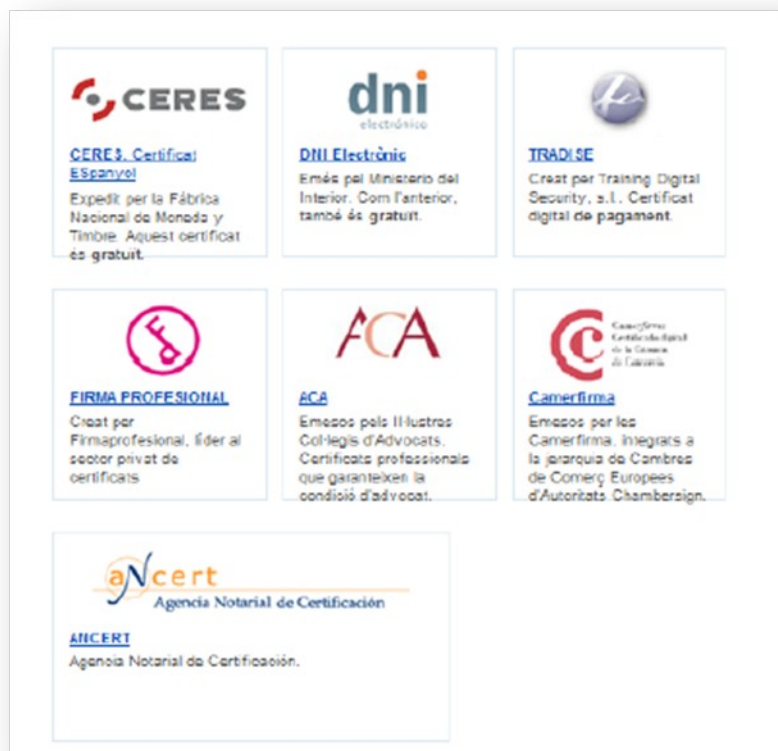


Figura 12: Autoritats de certificació.

L'AC disposa dels seus propis certificats amb els quals signa els certificats que emet organitzats de manera jeràrquica. Una jerarquia de certificació consisteix en una estructura jeràrquica d'AC en la qual es parteix d'una AC arrel, i a cada nivell existeix una o més AC que poden signar certificats d'entitat final.

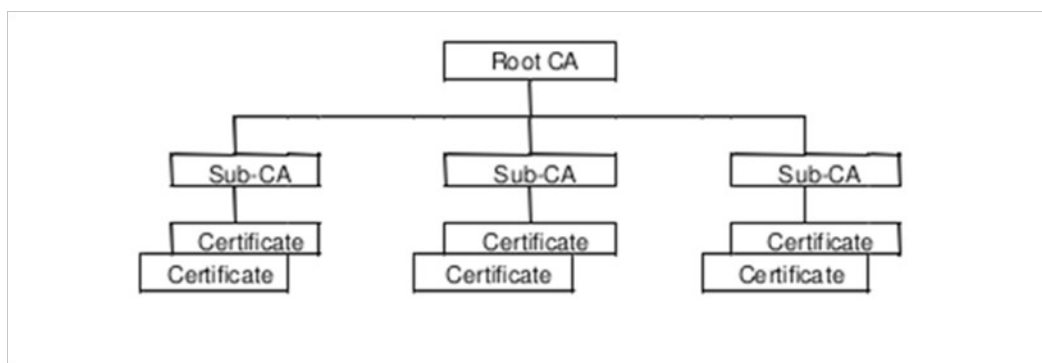


Figura 13: Jerarquia de certificació.

L'AC, per si mateixa o mitjançant la intervenció d'una Autoritat de Registre, verifica la identitat del sol·licitant d'un certificat abans d'expedir-lo.

Finalment, l'AC, mitjançant funcions criptogràfiques, crea el certificat a partir de les dades verificades anteriorment i garanteix, mitjançant una signatura electròni-

ca, la validesa del certificat creat. Si el certificat ha estat signat electrònicament per una AC, l'anomenem certificat reconegut.

2.1.3 Contingut d'un certificat electrònic

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

- **General:** es pot veure el nom del propietari del certificat i la data de validesa.
- **Detalls:** conté 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, aquesta cadena està formada per un certificat arrel que signa un certificat intermedi i aquest és el que s'utilitza per signar el nostre certificat.

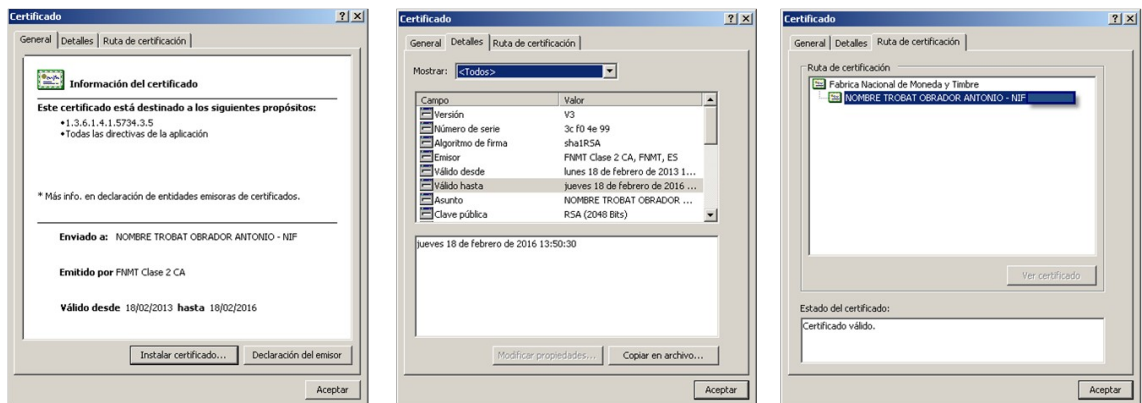


Figura 14: Informació de la clau pública del certificat electrònic.

Marc normatiu de signatura electrònica

L'article 10 de la Llei 39/2015 regula els sistemes de signatura electrònica que pot utilitzar l'interessat. Els sistemes de signatura electrònica han d'acreditar l'autenticitat de la signatura, com també la integritat i la inalterabilitat del document. Aquests sistemes de signatura són:

- **Sistemes de signatura 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 (Llei 40/2015), que regula la signatura electrònica del personal de les administracions públiques, diu que:

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

2.2 Conceptes bàsics de signatura electrònica

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

- Identifiquen el signant.
- Asseguren la integritat del document signat.
- Garanteixen el no-repudi en l'origen (el que ha signat no pot negar que hagi estat ell qui ha signat).

Per signar un document és necessari disposar d'un certificat digital o un DNI electrònic. Aquests contenen unes claus criptogràfiques (pública i privada) que són els elements necessaris per signar.

Aquestes claus són complementàries, això vol dir que tot allò que es xifra amb la clau privada només pot ser desxifrat amb la seva clau pública; per tant, podem saber sens dubte qui és l'emissor del missatge.

La clau privada s'emmagatzema en una targeta criptogràfica protegida per un pin i no es pot compartir. En canvi, la clau pública s'emmagatzema en el certificat electrònic del signant i es pot compartir.

2.3 Tipologia de signatura electrònica

Segons la normativa es distingeixen els tipus de signatura electrònica següents:

- **Signatura electrònica avançada.** És la signatura electrònica que està vinculada al seu signant de manera única i intransferible. Permet la seva identificació. Està basada sobre certificats electrònics, però no són certificats electrònics reconeguts o qualificats (emesos per una Autoritat de Certificació -AC). Garanteix l'autenticitat i integritat d'un document signat.
- **Signatura electrònica reconeguda o qualificada.** És la signatura electrònica avançada, però basada en un certificat electrònic reconegut o qualifi-

cat i està generada mitjançant un dispositiu qualificat de creació de signatures. **La signatura electrònica reconeguda o qualificada és l'única que es pot considerar equivalent a la signatura manuscrita.**

En resum, la signatura electrònica reconeguda o qualificada ha de:

1. Identificar el signant.
2. Verificar la integritat del document signat.
3. Garantir el no-repudi en l'origen (el que ha signat no pot negar que hagi estat ell qui ha signat).
4. Disposar de la participació d'un tercer de confiança (Autoritat de Certificació).
5. Estar basada en un certificat electrònic reconegut o qualificat.
6. Estar generada per un dispositiu qualificat de creació de signatures.

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

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 és el que signarà.

2.4 Sistema de signatura centralitzada: Cl@veFirma

2.4.1 Què és Cl@veFirma?

Cl@ve és un sistema d'identificació, autenticació i signatura electrònica per als ciutadans, basat en l'ús de claus concertades.

La principal novetat que incorpora el sistema Cl@ve és [Cl@veFirma](#), en què hi ha la possibilitat de signar mitjançant certificats electrònics centralitzats (certificats al núvol), és a dir, certificats electrònics emmagatzemats i custodiats per la Direcció General de Policia.

Aquests certificats centralitzats permeten al ciutadà signar documents electrònics des de qualsevol dispositiu que tingui connexió a Internet i sense cap equipament addicional.

Per utilitzar la signatura centralitzada, cal haver seguit prèviament els passos següents:

- **Registre de nivell avançat en el sistema Cl@ve:** es requereix registre al sistema, bé de manera presencial en una oficina davant d'un empleat pú-

blic habilitat, o bé de manera telemàtica, mitjançant un certificat electrònic reconegut o qualificat.

- **Activació de la Cl@ve Permanent:** obtenció de credencials d'accés al sistema mitjançant identificador d'usuari i contrasenya. Addicionalment, i quan el tipus de tràmit ho requereixi, es pot requerir una verificació addicional a través d'un codi d'un sol ús que s'envia al mòbil de l'usuari.
- **Generació del certificat de signatura:** aquesta acció es pot fer de manera automàtica en el moment de fer la primera signatura, o en qualsevol altre moment a voluntat de l'usuari.

2.4.2 Procés de signatura amb Cl@veFirma

Una vegada generat el certificat, aquest es pot emprar per signar documentació que requereixi signatura del ciutadà durant la tramitació electrònica d'un procediment administratiu.

Seguidament es presenta un exemple amb els passos d'aquest procés de signatura:

• Pas 1. Selecció del sistema Cl@veFirma

En aquest cas, la plataforma de tramitació telemàtica sol·licita la signatura electrònica d'un document del tràmit. Seleccionarem com a sistema de signatura Cl@veFirma.

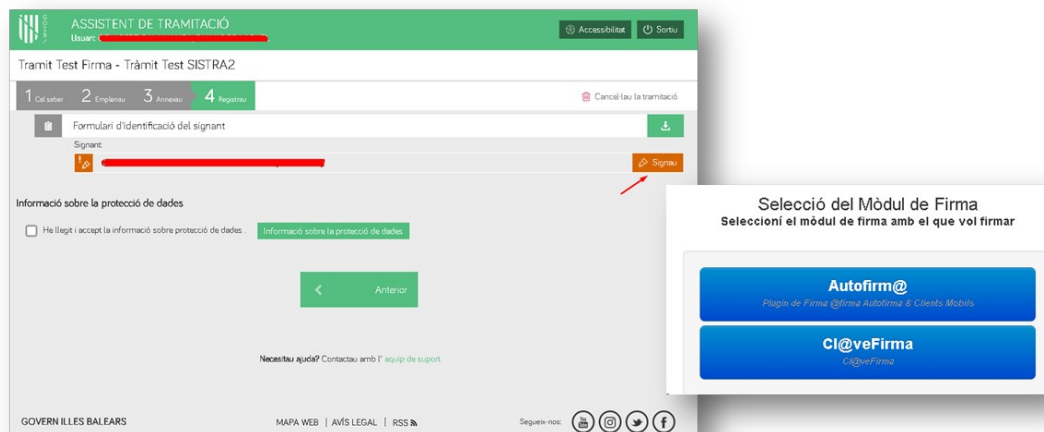


Figura 15: Selecció de Cl@veFirma.

• Pas 2. Selecció del certificat electrònic

L'assistent de signatura FIRE sol·licita llavors la selecció del certificat electrònic que s'empra per signar el document. En cas que el certificat no s'ha-

gi expedit, s'inicia automàticament el procés de generació i custòdia per part de la Direcció General de Policia.



Figura 16: L'assistent de signatura FIRE.

• Pas 3. Autenticació amb Cl@ve Permanent

Seguidament, el sistema requereix autenticació amb Cl@ve Permanent per poder usar el certificat. En aquest cas, se sol·licita un doble factor d'autenticació (contrasenya + codi SMS).



Figura 17: Autenticació amb Cl@ve permanent.

• Pas 4. Signatura del document

Finalment, el sistema signa el document i el retorna a l'assistent de tramitació.

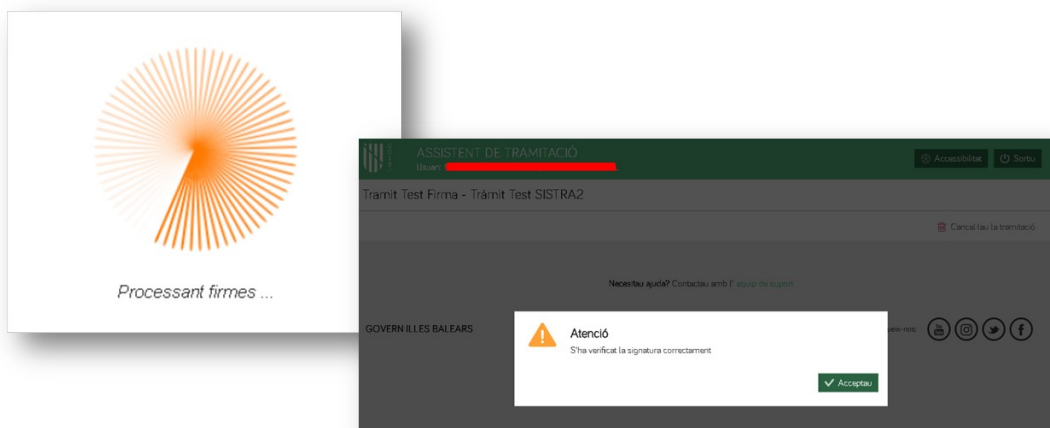


Figura 18: Procés de signatura d'un document durant l'execució d'un tràmit telemàtic.

2.4.3 Validar la signatura electrònica

Existeixen diversos mecanismes per validar un document signat electrònicament. En el cas d'un document amb la signatura incrustada, com és el cas dels PDF, el mateix visor de PDF porta una eina que permet validar la signatura.

La capacitat de validar d'aquesta eina varia; depèn de la versió del visor de PDF que hi ha instal·lat 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 19: Validador de la signatura electrònica d'Adobe Reader.

2.5 Validació i impressió de documents signats

2.5.1 Validar la signatura electrònica

Per això, és més recomanable utilitzar qualque servei qualificat per validar la signatura. Per exemple, podem fer servir el servei VALIDE de validació de certificats i signatura electrònica, que permet una validació completa de la signatura.

<https://valide.redsara.es>

The screenshot shows the VALIDE website interface. At the top, there's a header with the 'gob.es' logo, the 'VALIDE' logo, and navigation links: 'Bienvenido | Benvingut | Ongi etorri | Benvido | Welcome'. There's also a 'Contactar' button and a Spanish flag icon. The main content area is titled 'Validar Firma' and includes a sub-header: 'Puedes comprobar la validez de una firma digital utilizando para ello la plataforma @firma.' Below this, there are two main steps: 1. 'Selecciona la firma a validar' with a 'Navega...' button and a message 'No s'ha seleccionat cap fitxer.' and 2. 'Introduce el código de seguridad' with a text input field and a 'Validar' button. A note at the bottom states: 'Nota: Las firmas soportadas por el sistema son aquellas que han sido realizadas con los certificados admitidos por el Ministerio de Industria, Energía y Turismo. Se pueden consultar los certificados admitidos revisando el documento Certificados admitidos por la plataforma @firma. Si tu firma no se valida correctamente, porque se indica certificado no soportado, pero tu certificado si se encuentra entre los recogidos en la Página del Ministerio de Industria te rogamos te pongas en contacto con el servicio de soporte.'

Figura 20: Interfície gràfica de Valide.

2.5.2 Imprimir un document signat

La impressió d'un document signat per una administració ha de proporcionar alguna manera de poder validar que el document original que té l'administració sigui el mateix que està imprès.

Per això, el procés d'impressió del document signat reflecteix en el document en paper, a part del contingut del document, la informació següent:

- **Codi segur de verificació (CSV)**, per a la seva verificació posterior a la seu electrònica.
- **Dades de representació de la signatura.**

L'exemplar imprès del document electrònic constitueix el justificant de signatu-

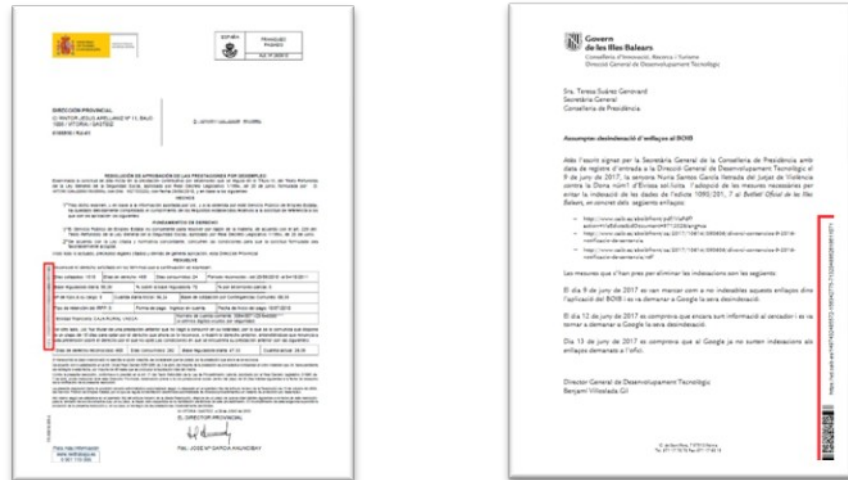


Figura 21: Document signat amb CSV.

ra del document electrònic.

El CSV ha de ser únic i està 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 s'anomena CONCSV i està disponible a la Seu Electrònica (<https://csv.caib.es>).



Figura 22: Interfície gràfica de CONCSV.

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

3. Sistemes de representació

L'article 5 de la Llei 39/2015 defineix els mecanismes de representació i els mitjans necessaris per acreditar-la.

Els interessats amb capacitat d'actuar ho poden fer amb les administracions públiques mitjançant representant, a excepció de manifestació expressa en contra per part de l'interessat.

Les persones físiques i jurídiques (sempre que ho prevegin els seus estatuts) poden actuar en representació d'altres davant l'Administració.

S'ha d'acreditar la representació per formular sol·licituds, presentar declaracions responsables o comunicacions, interposar recursos, desistir d'accés i renunciar a drets en nom d'una altra persona.

Per a aquells actes que siguin de tràmit, se'n presumeix la representació.

La representació es pot acreditar mitjançant la inscripció en el Registre d'apoderaments de l'Administració pública o organismes competents.

3.1 Registre electrònic d'apoderaments

Segons preveu l'article 6 de la Llei 39/2019, l'Administració General de l'Estat, les comunitats autònomes i les entitats locals disposen d'un registre electrònic d'apoderaments i, en l'àmbit estatal, aquest registre és el **Registre electrònic d'apoderaments** de l'AGE.

La Comunitat Autònoma de les Illes Balears està adherida a aquest registre, que s'ha de considerar el Registre electrònic d'apoderaments de la Comunitat Autònoma.

3.2 Registre de funcionaris habilitats

La Llei 39/2019 preveu que l'Administració General de l'Estat, les comunitats autònomes i les entitats locals hagin de mantenir actualitzat un registre, o un altre sistema equivalent, en què constin els funcionaris habilitats.

Aquests registres o sistemes han de ser plenament interoperables i estar interconnectats amb els de la resta d'administracions públiques, a l'efecte de comprovar la validesa de les habilitacions.

En aquest registre o sistema equivalent han de constar almenys els funcionaris que prestin serveis a les oficines d'assistència en matèria de registre (article 12) i, si escau, aquells funcionaris que tinguin habilitació per efectuar còpies autèntiques, de manera que es garanteixi que aquestes s'han expedit adequadament (article 27).

Així doncs, el ciutadà (persona física) que vulgui ser assistit per un funcionari habilitat ha de:

- Identificar-se davant el funcionari habilitat.
- Presentar consentiment exprés per cada procediment iniciat pel funcionari, fet del qual en queda constància dins l'expedient administratiu.

3.3 Plataforma d'habilitació de professionals

Tot i que encara no està integrat dins els sistemes d'administració electrònica de la CAIB, es preveu consultar i validar les habilitacions mitjançant el sistema Representa.

A través de Representa es pot:

- Comprovar si un representant pertany o no a un col·lectiu professional.
- Comprovar si el representant/col·lectiu està adherit a un determinat conveni que l'habilita a realitzar tràmits.
- Obtenir una llista dels tràmits administratius que pot dur a terme un representant pel fet de pertànyer a un col·lectiu adherit.
- Comprovar l'estat (actiu/inactiu) del representant dins del seu col·lectiu professional, i si pertany a algun subcol·lectiu.

Entre els col·lectius adherits destaquen el Consell de Gestors Administratius i el Consell Oficial de Graduats Socials, com també els col·legis professionals respectius que hi estiguin adherits.

Encara que a dia d'avui no estigui integrada amb els sistemes d'administració electrònica, la Comunitat Autònoma de les Illes Balears preveu consultar i validar les habilitacions mitjançant el sistema Representa.

A continuació, es mostra una figura que reflecteix la integració de Representa en altres eines de l'administració electrònica.

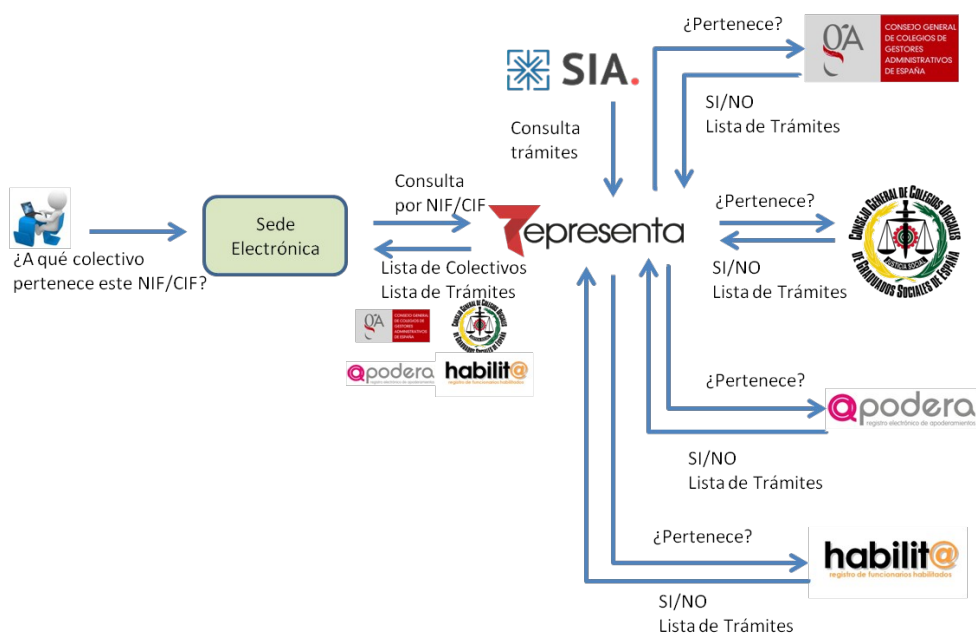


Figura 23: Integracions de Representa en altres eines d'administració electrònica.

BIBLIOGRAFIA

Acord de Consell de Ministres, de 19 de setembre de 2014, pel qual s'aprova Cl@ve, la plataforma comuna del Sector Públic Administratiu Estatal per a la identificació, autenticació i firma electrònica mitjançant l'ús de claus concertades: <https://www.boe.es/buscar/doc.php?id=BOE-A-2014-10264>

Component Horitzontal d'Autenticació de la CAIB (LOGINIB): <https://www.caib.es/sites/administracioidigital/ca/eines-52113/>

Criptografia asimètrica: https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica

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

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

Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques: <https://boe.es/buscar/act.php?id=BOE-A-2015-10565>

Passarel·la d'Autenticació Cl@ve: https://clave.gob.es/clave_Home/clave.html

Presentació general sobre el sistema Cl@ve: <https://administracionelectronica.gob.es/ctt/resources/Soluciones/766/Descargas/Clave-Identificacion.pdf?idIniciativa=766&idElemento=12264>

Procés de signatura electrònica: https://arturomesc.files.wordpress.com/2012/10/proceso_firma_electronica.png

Registre de funcionaris habilitats: <https://administracionelectronica.gob.es/ctt/resources/Soluciones/747/Descargas/Presentacion-HABILITA.pptx?idIniciativa=747&idElemento=12750>

Registre Cl@ve: https://clave.gob.es/clave_Home/registro/Como-puedo-registrarme.html

Reglament UE 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014R0910&from=IT>

Reial decret 3/2010, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-1330

Seu Electrònica de la CAIB: <https://www.caib.es/seucaib>

Sistema de signatura electrònica centralitzada Cl@veFirma: https://clave.gob.es/clave_Home/dnin/queEs.html



GOIB
/

Validació de signatura electrònica: <https://valide.redsara.es/valide/validarFirma/ejecutar.html>