

The logo for 'idigital' is displayed in a bold, blue, sans-serif font. The letters 'i', 'd', and 'i' are stylized with vertical bars through them, suggesting a digital or networked theme.

**Generalitat  
de Catalunya**

# Administració electrònica. Agilitza els tràmits amb l'administració

L'administració electrònica permet dur a terme tràmits amb l'Administració a través d'Internet, és a dir, en qualsevol lloc i a qualsevol hora. Elements com la signatura digital o l'eDNI (i l'IdCAT a Catalunya) garanteixen la seguretat, validesa i representació legal de les gestions en línia.

## DESCRIPCIÓ

Davant la necessitat de les empreses i també dels ciutadans d'interactuar amb l'Administració pública, i gràcies a la universalització de l'accés d'Internet, els governs, a través de les seves entitats administratives, promouen l'**administració electrònica**. D'aquesta manera les empreses disposen d'una plataforma que els permet realitzar tràmits d'una manera electrònica utilitzant Internet.

Per això s'està desenvolupant una plataforma que disposarà dels últims avenços tecnològics, que permeten l'ús de formularis anomenats intel·ligents, signatures electròniques, emissió de certificats administratius signats per l'administració i també la capacitat de la presentació "no presencial" i en temps real de qualsevol documentació de forma electrònica.

L'administració electrònica aporta una millora funcional que li permet prestar un millor servei, millorar la seva imatge i esdevenir una eina imprescindible sense ser feixuga per a les empreses i els ciutadans. Les millores funcionals que aporta són les següents:

- Creació d'un únic espai web amb prestació de serveis 24 hores al dia i 7 dies a la setmana, de manera els usuaris que accedeixin als serveis de l'administració electrònica es trobaran sempre amb el mateix entorn disponible a tot arreu on es pugui accedir a Internet.
- Integració dels serveis públics en paquets, agrupats segons les necessitats del ciutadà o empresa.
- Tramitació digital de la informació.
- Increment de la seguretat amb l'objectiu de generar confiança als usuaris no presencials.
- Accés a la informació sobre el desenvolupament i l'estat de qualsevol tramitació en curs. També accés a les dades del ciutadà o empresa gestionades durant la tramitació, tant si s'adquireixen directament com si s'obtenen d'altres administracions.
- Facilitat d'intercanvi entre administracions, permetent que les dades flueixin sense intervenció del ciutadà, fent que aquestes siguin el més fidedignes i precises.

Ara bé, l'administració electrònica per poder incorporar aquestes funcionalitats, necessàriament s'ha de recolzar sobre diversos punts tecnològics:

- Disponibilitat d'una infraestructura de clau pública, explicada a continuació, que fa possible l'autenticació de les transaccions de dades mitjançant la signatura digital.
- Desenvolupament de les aplicacions segons una arquitectura amb un potent sistema de seguretat, per tal de garantir la independència de les dades en relació amb el sistema i la seva utilització. Això facilita la consulta de forma fiable i confidencial als ciutadans i empreses a través dels portals facilitats per l'administració electrònica.

- I també fruit de l'arquitectura segura de les aplicacions, es permetrà el reaprofitament de les dades certificades per poder ser enviada entre administracions que actualment estan, incomunicades. Aquest punt permetrà a molts ciutadans, i sobretot a les empreses, alleugerir notablement els tràmits burocràtics que consisteixen a traslladar un coneixement propietat d'una administració a una altra.

Es considera un factor vital dotar l'administració electrònica de mecanismes que permetin que tingui igual validesa un tràmit presencial que un no presencial, aportant seguretat a les gestions fetes telemàticament. De manera que s'incorpora la infraestructura de clau pública, que és suficientment unívoca i segura per ésser la tecnologia que permeti la interacció digital amb l'administració.

Aquesta infraestructura de clau pública és el que coneixem com a **Signatura digital**. La Signatura digital és un mètode criptogràfic que associa la identitat d'una persona o d'un equip informàtic a un missatge o document concret. En funció del tipus de signatura (segons el nivell de seguretat o certificats que incorpora), pot, addicionalment, assegurar la integritat del document o missatge.

La signatura digital o electrònica, com la signatura autògrafa (manuscrita), es pot vincular a un document per identificar-ne l'autor, per establir conformitat (o disconformitat) amb el contingut, per indicar que s'ha llegit o, segons el tipus de signatura, garantir que no es pugui modificar el seu contingut.

A nivell tècnic, la signatura digital es basa en criptografia de clau pública. En aquest tipus de criptografia cada usuari té un parell de claus: una pública i una privada. La clau pública es distribueix lliurement, però la clau privada és secreta i no és deduïble a partir de la clau pública. Per crear una signatura digital són necessaris tres processos o algorismes criptogràfics: un per generar la clau, un per signar i l'altre per verificar la signatura.

Per exemple, quan l'empresa A necessita enviar un missatge a l'empresa B i vol que el receptor estigui segur que el missatge prové d'ells es segueixen els següents passos: A envia el seu missatge a B i adjunta una signatura digital. Aquesta signatura es genera usant la clau privada d'A i pren la forma d'un valor numèric. En rebre el missatge, l'empresa B pot confirmar la procedència del missatge utilitzant la clau pública de l'empresa A, prèviament subministrada. Si la verificació és correcta l'empresa B pot estar segura que el missatge procedeix de l'empresa A ja que l'algorisme de signat està dissenyat per tal que sigui molt difícil crear una signatura que encaixi amb un missatge concret (sinó es coneix la clau privada).

La signatura digital es basa en una jerarquia de confiança. És a dir, existeixen un sèrie d'autoritats de certificació (AC o CA de les sigles en anglès "Certification Authority"), que són unes entitats de confiança responsables d'emetre i revocar els certificats digitals utilitzats en la signatura electrònica. Per

això el receptor d'un document signat digitalment confia en el sotasignat perquè ha utilitzat una signatura digital emesa per una autoritat de confiança de la qual n'accepta els seus certificats. Per exemple, la Agència Catalana de Certificació (CATCert) i la Fàbrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT) són autoritats de certificació homologades a nivell mundial (compleixen unes directrius legals i de qualitat degudament provades) i per tant poden emetre certificats digitals, com per exemple l'IdCat o bé l'eDNI, entre d'altres. Per altra banda s'ha de tenir en compte que les administracions públiques estatals només accepten les signatures digitals emeses per CATCert i la FNMT, en concret l'IdCAT i l'eDNI. És a dir, una empresa que disposa d'una signatura digital emesa per Thawte (entitat homologada com a CA) no la podrà utilitzar per realitzar tràmits d'administratius a les administracions electròniques estatals.

Per tant, les empreses que vulguin interactuar amb l'administració electrònica hauran de disposar de signatura electrònica homologada. Per això, en l'àmbit català existeix l'**IdCAT**, i en l'àmbit estatal l'**eDNI**. Tant una com l'altra són igual d'aptes per interactuar amb qualsevol de les administracions d'àmbit estatal (administracions central, autonòmica i local).

A efectes pràctics una signatura digital no deixa de ser un petit fitxer digital (un arxiu informàtic) que conté les dades necessàries per les seves funcions. I això existeix tant en l'IdCAT com a l'eDNI, ara bé, la principal diferència entre una i l'altra, és que l'IdCAT no està plantejat perquè estigui en cap mena de suport físic específic (tot i que es pot subministrar l'IdCAT a través d'una clau de memòria USB), mentre que l'eDNI sí. Si es sol·licita d'IdCAT, al final rebrem per correu electrònic el fitxer que conté els certificats per dur a terme la signatura digital, mentre que en l'eDNI, aquest fitxer està contingut en el xip que incorpora el nou document nacional d'identitat.

Per això, l'eDNI no deixa de ser el DNI de sempre que incorpora un xip, que a més d'altres coses (dades del ciutadà o empresa, caducitat del document, fotografia digital, etc.), conté la signatura digital. D'aquesta manera, a través de terminals lectors de targetes homologats per l'administració pública es pot utilitzar l'eDNI per signar, tramitar o consultar dades dels tràmits fets de forma individual i confidencial pel ciutadà o empresa.

L'**idCAT** és un identificador digital que garanteix la identitat de les persones a Internet. Permet operar amb diferents administracions i, a més, assegura la integritat de les dades que s'envien, així com la seva confidencialitat, ja que està emès per l'**Agència Catalana de Certificació - CATCert**. També permet fer altres operacions, com ara signar correus electrònics, documents electrònics (per exemple, fitxers en format PDF) i formularis web (per exemple, les declaracions que les empreses fan a l'Agència Tributària). Sense la signatura electrònica els tràmits telemàtics no tenen validesa, ja que la xarxa electrònica no ofereix el nivell de seguretat necessari per garantir les dades de l'empresa o ciutadà.

Hi ha tres motius per utilitzar signatures digitals en les comunicacions:

- Autenticitat: Un sistema criptogràfic de clau pública permet a qualsevol persona enviar missatges utilitzant una clau pública. La signatura permet al receptor d'un missatge estar segur que el remitent és qui diu que és.
- Integritat: Emissor i receptor voldran estar segurs que el missatge no s'ha alterat durant la transmissió.
- No-repudiació: En un context criptogràfic, la paraula repudiació fa referència a l'acció de negar la relació amb un missatge (per exemple, dient que ha estat enviat per un tercer). El receptor d'un missatge pot insistir que l'emissor envii adjunta una signatura per prevenir que més endavant l'emissor pugui repudiar el missatge, així el receptor pot mostrar el missatge a un tercer i provar-ne l'origen.

Amb la Llei 59/2003, de 19 de desembre, de signatura electrònica, l'eDNI, el DNI electrònic, es converteix en una realitat. Amb aquest nou document d'identitat es persegueixen diversos avantatges:

- Creació d'un document que certifiqui la identitat del ciutadà en totes les tramitacions electròniques, i que permeti signar tot tipus de documents electrònics. Fent servir un dispositiu segur de creació de signatura, la signatura electrònica que s'efectuï mitjançant el DNI electrònic tindrà efectes equivalents als d'una signatura manuscrita.
- Expedició del DNI electrònic en un sol acte administratiu, cosa que redueix el temps empleat per a la seva obtenció.
- Acceptació per part de totes les administracions públiques. (Per exemple, per tramitar la declaració de la renda, per demanar un certificat d'empadronament, per donar-se d'alta al registre de naixements o per reclamar el dret a una pensió.)
- Aquest certificat està incorporat al DNI, i a més d'identificar el ciutadà (autenticació), garanteix que la informació no ha estat alterada (integritat) i que el ciutadà ha realitzat la transacció (no-repudiació).

L'eDNI l'emet i el valida la FMNT, el Ministeri d'Administracions Públiques a través del conjunt d'administracions públiques i l'entitat pública empresarial Red.es.

Si una empresa o un ciutadà disposa d'una signatura digital pot accedir als serveis de les diferents administracions públiques, que són:

- Ajuntaments
- Consorci de l'Administració Oberta de Catalunya (CAOC)
- Generalitat de Catalunya
- Diputacions provincials
- Ministeris del Govern d'Espanya
  - Ministeri d'Economia i Hisenda (Agència Estatal d'Administració Tributària, Direcció General de Cadastre i Institut Nacional d'Estadística)
  - Ministeri d'Indústria, Turisme i Comerç
  - Ministeri de Foment

- Ministeri d'Administracions Públiques
- Ministeri de Cultura
- Ministeri de l'Interior (DGT)
- Agència Espanyola de Protecció de Dades
- Ministeri de Treball i Assumptes Socials (Seguretat Social i INEM)

Actualment ja hi ha molts serveis en línia disponibles per a una empresa, però de mica en mica es van ampliant fins a arribar a la totalitat dels tràmits administratius. Per exemple, aquests són alguns dels serveis als quals es pot accedir amb l'IdCAT i l'eDNI:

- Declaració i/o canvi de domicili fiscal d'una empresa
- Consulta de l'estat dels tràmits
- Presentació de l'escrit d'al·legacions contra denúncies
- Consulta de la titularitat dels impostos, taxes i preus públics de béns immobles (IBI), vehicles de tracció mecànica (IVTM), etc.
- Servei d'Ocupació de Catalunya (SOC) i INEM per realitzar gestions per contractacions
- Identificació en el portal per accedir als serveis com a demandants d'ocupació
- Tributs i multes pendents de pagament
- Tributs i multes pagades
- Expedients executius de tributs i multes
- Correcció de dades de l'empresa
- Presentació de declaracions i consultes (entre altres la presentació de la declaració de la renda)
- Altres declaracions i liquidacions de l'Agència Tributària
  - Retencions d'IRPF a càrrec de l'empresa
  - Liquidació d'IVA
  - Impost de societats
  - Resums anuals
  - Declaracions d'operacions intracomunitàries
  - Etc.
- Duanes i impostos especials
- Pagament d'impostos mitjançant un formulari validat amb la signatura digital
- Pagament de deutes
- Constitució i devolució de dipòsits
- Informe de vida laboral dels treballadors
- Sol·licitud de rectificació de l'informe de vida laboral
- Informe de bases de cotització règim general i mar
- Sol·licitud de rectificació informe de bases de cotització
- Situació laboral actual
- Duplicat del document d'afiliació
- Sol·licitud de canvi de base de cotització (per a autònoms)
- Consulta de l'estat d'una prestació

A més de tots aquests serveis, disposar d'una signatura digital permet:

- Signar correus electrònics
- Encriptar correus electrònics
- SignaCAT (signatura i encriptació de fitxers)
- Formsign (signatura de formularis web)

La signatura digital s'incorporarà en molts tràmits que es realitzen no tan sols amb l'Administració pública, sinó també dins del món empresarial per poder identificar, verificar i acceptar accions que es produeixin dins de l'entramat de processos empresarials. Per exemple, atorgar poders, rubricar un acord entre socis, aprovar un pressupost, validar un contracte, etc. Per tant, de mica en mica, la signatura manuscrita s'anirà substituint per la signatura digital. Això farà que no puguin existir mai ambigüitats en la signatura i s'incorpora un mecanisme digital més a tots els que ja existeixen dins de l'empresa.

## AVANTATGES

Els principals avantatges de l'administració electrònica i la signatura digital són:

- Permet un estalvi de temps molt important de cara a realitzar tràmits purament administratius de l'empresa.
- Millora l'eficiència en les tramitacions.
- Permet signar correus electrònics i altres documents (PDF, declaracions, etc.).
- Proporciona un certificat digital per altres usos futurs: comerç electrònic, banca electrònica, etc.
- Substitueix la signatura autògrafa per la digital, de manera que és un pas més cap a la digitalització.
- Proporciona integritat: l'emissor i el receptor estan segurs que el missatge no s'ha alterat durant la transmissió.
- Proporciona autenticitat: la signatura permet al receptor d'un missatge estar segur que el remitent és qui diu que és.
- Permet la no-repudiació: el receptor d'un missatge pot insistir que l'emissor enviï adjunta una signatura per prevenir que més endavant l'emissor pugui repudiar el missatge. En un futur, i per arribar a les oficines sense papers, totes les documentacions que requereixin signatura es faran a través de signatures digitals.
- Permet la interoperabilitat amb els projectes europeus d'identificació digital.



## COSTOS

Obtenir l'IdCAT és totalment **gratuït** accedint a idCAT.

Obtenir l'eDNI és totalment **gratuït**.

## CLAUS

Passos que cal seguir per obtenir d'IdCAT:

- Accedir a l'IdCAT a través del web [www.idcat.net](http://www.idcat.net).
- Entrar les dades personals i la resta de dades requerides.
- Localitzar una oficina d'una entitat de registre on es puguin acabar de fer els tràmits (gestió presencial).
- Sol·licitar el certificat a través del web.
- Accedir personalment a una entitat de registre on, si cal, s'haurà d'acreditar la identitat i altres dades que siguin necessàries.
- Un cop validat, es rebrà un correu que contindrà el certificat de la signatura digital.
- Instal·lar el certificat en el mateix ordinador on s'han fet tots aquests tràmits.
- S'aconsella fer una còpia de seguretat del certificat per si cal utilitzar-lo en altres ordinadors o per si s'extravia.

Passos que cal seguir per obtenir l'eDNI:

- Qui sol·liciti per primera vegada l'eDNI i, per tant, els certificats electrònics associats (guardats dins del xip), haurà d'anar a una oficina d'expedició de l'eDNI.
- Per sol·licitar l'expedició de l'eDNI és imprescindible la presència física de la persona a qui se li hagi d'expedir, l'abonament de la taxa establerta legalment en cada moment i la presentació dels documents necessaris.
- El lliurament de l'eDNI i dels certificats associats es realitzarà personalment al seu titular el mateix dia en què se'n sol·liciti l'expedició.
- Un cop finalitzada la fase de gestió documental i la personalització física de la targeta, comença la fase de personalització lògica amb la càrrega de dades al xip de la targeta suport. La generació de claus es realitzarà a la targeta i en presència del titular, després de l'habilitació d'un PIN aleatori que es lliura en un sobre cec.

És important que un ciutadà o una empresa conegui els passos a seguir per obtenir una signatura digital.

Cal assabentar-se de les prestacions que té la signatura digital. És important saber en quins llocs es pot utilitzar.

És imprescindible tenir un mínim de precaucions quan es disposa d'una signatura digital. Evidentment un certificat digital en males mans pot fer molt de mal i, per tant, s'han de seguir uns consells mínims de seguretat: tenir còpies de seguretat de la signatura, verificar la data de caducitat (en cas que caduqui), verificar que si s'instal·la en un ordinador només hi podrà accedir el titular de la signatura, mantenir en un lloc segur el PIN (si és necessari), tenir controlades les còpies o els documents de la signatura digital, etc.

En cas de pèrdua o possible ús fraudulent d'una signatura digital, és important donar-la de baixa i tramitar els tràmits consegüents (denúncia, anul·lacions d'operacions, etc.)

## PROVEÏDORS

Si vols obtenir informació de quines empreses poden desenvolupar aquesta solució consulta el [MapaTIC](#), un catàleg digital d'empreses TIC catalanes.

## GLOSSARI

### Certificat digital

És un document digital que incorpora una clau pública mitjançant el qual un tercer en qui es confia (una autoritat de certificació) garanteix la vinculació entre la identitat d'un subjecte o entitat i la seva clau pública. Tipus de certificats: personal, d'adscripció a una empresa, representant, persona jurídica, d'atribut, de servidor segur, firma de codi, etc.

### Clau pública i privada

Són les claus que es fan servir en un mètode criptogràfic per l'enviament de missatges. Les dues pertanyen a la mateixa persona a qui s'ha enviat un missatge. Una clau és pública i es pot lliurar a qualsevol persona. L'altra és privada i el propietari l'ha de guardar de manera que ningú no hi tingui accés. El remitent fa servir la clau pública del destinatari per xifrar el missatge i, un cop xifrat, només la clau privada del destinatari podrà desxifrar el missatge.

### Entitat certificadora

És l'encarregada d'emetre i revocar certificats. És l'entitat de confiança que dona legitimitat a la relació d'una clau pública amb la identitat d'un usuari o servei.

### Hash criptogràfic

És el mètode per generar claus que representen de manera gairebé unívoca un document, registre, fitxer, etc.

### PIN

També anomenat clau personal d'accés. És una seqüència de caràcters que permet l'accés als certificats, aplicacions o sistemes d'informació.