PARLAMENT DE CATALUNYA

Política d'identificació, signatura electrònica, segells electrònics i certificats del Parlament de Catalunya

395-00054/15

Versió 1.0

Data: Desembre 2025

Descripció de la Política	
Nom del document:	Política d'identificació, signatura electrònica, segell electrònics i certificats del Parlament de Catalunya
Versió:	v.1.0
URi:	BOPC 386/15, T 24.12.2025
Data d'aprovació:	9/12/2025
Àmbit d'aplicació:	Aquesta política és aplicable a la documentació del Parlament fruit de les actuacions que li són pròpies, tant les parlamentàries com les que són sotmeses al dret administratiu, i també a les aplicacions corporatives. La PISEC és aplicable a totes les persones que interactuen amb el Parlament, inclosos els diputats. També és aplicable pel que fa a les relacions per mitjans electrònics amb tercers, ja siguin persones físiques o jurídiques.
Identificació del gestor:	A09006440
Contacte	
Responsable:	Àrea d'Arxiu i Gestió Documental del Departament de Gestió Documental i Recursos d'Informació.
Adreça electrònica:	arxiu@parlament.cat

SUMARI

Introducció 5

1. Objectiu 6

2. Àmbit d'aplicació 6

3. Sistemes d'identificació i signatura electrònica del Parlament de Catalunya 6

3.1. Sistemes d'identificació 7

3.1.1. Persones físiques 7

3.1.2. Persones jurídiques o ens sense personalitat jurídica 7

3.2. Sistemes de signatura 7

3.2.1. Persones físiques 7

3.2.2. Persones jurídiques i ens sense personalitat jurídica 8

3.3. Segells de temps 8

3.4. Identificació i signatura dels representants 8

4. Nivell de seguretat 9

4.1. Nivell de seguretat alt 10

4.2. Nivell de seguretat substancial 10

4.3. Nivell de seguretat baix 10

4.4. Nivells de seguretat associats als procediments parlamentaris 11

5. Aprovació i manteniment de la Política d'identificació, signatura electrònica, segells electrònics i certificats 12

5.1. Responsables que han de garantir l'aplicació de la Política d'identificació, signatura electrònica, segells electrònics i certificats 12

6. Període de validesa 13

7. Gestió i manteniment 13

8. Normativa i referències 14

Annex 1. Catàleg de sistemes d'identificació i signatura 15

A) Mecanismes no operats pel Parlament 15

B) Mecanismes operats pel Parlament 16

C) Descripció dels sistemes d'identificació i signatura 16

D) Actualització dels sistemes d'identificació i signatura electrònica 17

Annex 2. Mecanismes d'identificació i signatura per nivell de seguretat..... 18

A) Mecanismes d'identificació per nivell de seguretat 18

B) Mecanismes de signatura per nivell de seguretat 18

C) Actualització de la relació entre els nivells de seguretat i els mecanismes d'identificació 18

Annex 3. Glossari..... 19

Introducció

En el marc del procés d'implantació d'una administració parlamentària plenament digital, el Parlament de Catalunya s'ha de dotar d'una sèrie d'instruments que, de manera transversal, donin robustesa i seguretat als sistemes d'informació, aportin garantia jurídica a les tramitacions electròniques i compleixin amb la normativa en matèria d'Administració digital.

La Política d'identificació, signatura electrònica, segells electrònics i certificats és l'instrument per mitjà del qual es dota el Parlament d'un conjunt de regles i criteris comuns que determinen els sistemes d'identificació i signatura electrònica en aquesta institució, i compleix amb l'exigència per a les administracions públiques de disposar d'una política de signatura electrònica, establerta, entre altres disposicions normatives, per l'article 18.2 del Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema nacional d'interoperabilitat en l'àmbit de l'Administració electrònica. Cal esmentar que l'aprovació d'una nova versió de l'Esquema nacional de seguretat (ENS) per mitjà del Reial decret 311/2022, de 3 de maig, incorpora novetats en els diversos nivells de signatura electrònica establerts.

El Parlament de Catalunya aprova la Política d'identificació, signatura electrònica, segells electrònics i certificats d'acord, també, amb la Resolució de 27 d'octubre de 2016 de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Norma tècnica d'interoperabilitat de política de signatura i segell electrònics i de certificats de l'Administració (en endavant, NTI), que està alineada amb el 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 al mercat interior (en endavant, ReIDAS), i la Decisió d'execució (UE) 2015/1506 de la Comissió, de 8 de setembre de 2015, per la qual s'estableixen les especificacions relatives als formats de les signatures electròniques avançades i els segells avançats que han de reconèixer els organismes del sector públic, de conformitat amb els articles 27, apartat 5, i 37, apartat 5, del Reglament (UE) 910/2014.

A més, la Política d'identificació, signatura electrònica, segells electrònics i certificats inclou també la regulació dels sistemes d'identificació i signatura propis del Parlament de Catalunya que, tot i no estar especificats en la NTI, compleixen la normativa vigent, com codis segurs de verificació (CSV), claus concertades amb registre previ, etc.

L'evolució constant dels serveis digitals i de les tecnologies que en són el suport requereix sistemes àgils d'actualització per a garantir la vigència d'aquesta política. Per aquest motiu, es determina en l'annex 1, apartat *d*, d'aquest document la forma d'actualització i de publicitat del catàleg que aquesta política inclou.

1. Objectiu

La Política d'identificació, signatura electrònica, segells electrònics i certificats (en endavant, PISEC) té per objectiu establir el conjunt de criteris comuns adoptats pel Parlament amb relació a l'autenticació i el reconeixement de signatures electròniques, basades tant en certificats electrònics com en altres sistemes alternatius.

La PISEC estableix les directrius que el Parlament de Catalunya ha de seguir per a dotar de cobertura jurídica el desenvolupament dels procediments administratius i parlamentaris amb relació a l'ús de la signatura electrònica en les aplicacions corporatives, a fi de garantir l'autenticitat, la integritat i la conservació dels documents signats electrònicament. És aplicable tant a les signatures com als segells electrònics.

La PISEC inclou les identitats digitals i els certificats digitals de ciutadans i de tercers que el Parlament de Catalunya accepta i els certificats digitals que utilitzen els treballadors i els diputats del Parlament. En aquest últim cas, també se n'estableix el cicle de vida.

La PISEC descriu també els sistemes d'identificació i de signatura propis del Parlament de Catalunya basats en les evidències electròniques.

2. Àmbit d'aplicació

La PISEC és aplicable a la documentació del Parlament fruit de les actuacions que li són pròpies, tant les parlamentàries com les que són sotmeses al dret administratiu, i també a les aplicacions corporatives.

La PISEC és aplicable a totes les persones que interactuen amb el Parlament, inclosos els diputats. També és aplicable pel que fa a les relacions per mitjans electrònics amb tercers, ja siguin persones físiques o jurídiques.

3. Sistemes d'identificació i signatura electrònica del Parlament de Catalunya

Els sistemes d'identificació i signatura electrònica per a acreditar la identitat d'usuaris i signataris per mitjans electrònics es determinen en funció del subjecte, el grau de seguretat que requereixi el tràmit i el resultat del judici de proporcionalitat del sistema des del punt de vista de la normativa de protecció de dades.

3.1. Sistemes d'identificació

3.1.1. Persones físiques

S'admeten els sistemes d'identificació següents, enumerats en l'annex 1 d'aquest document:

- Els certificats electrònics qualificats que hagin estat emesos per prestadors de serveis de certificació (PSC) inclosos en la llista de confiança de prestadors de serveis de certificació, anomenada Trusted Services List (en endavant, TSL), publicada per l'òrgan competent de qualsevol país de la Unió Europea d'acord amb el que estableix el ReIdAS.
- S'ha d'admetre, amb caràcter general, qualsevol dels mitjans d'identificació inclosos en la llista que publica la Comissió Europea per a accedir als serveis prestats en línia per un organisme del sector públic en un estat membre, a l'efecte de l'autenticació transfronterera, d'acord amb el que estableix el ReIDAS.
- Amb l'entrada en vigor de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, s'admeten també altres mecanismes d'identificació i signatura electrònica de persona física no criptogràfics, més enllà dels certificats digitals, com són els basats en l'enviament de codis d'un sol ús a dispositius mòbils i amb un registre previ o qualsevol altre sistema amb registre previ, sempre que ho estableixi expressament la normativa reguladora aplicable.
- Els mecanismes emprats per a la identificació de persones físiques que autentiquin la identitat d'un ciutadà que declara representar una persona física.

3.1.2. Persones jurídiques o ens sense personalitat jurídica

S'admeten els sistemes d'identificació següents, enumerats en l'annex 1 d'aquest document:

- Els certificats de segell electrònic qualificat emesos a favor d'una persona jurídica o un ens sense personalitat per prestadors de serveis de certificació (PSC) inclosos en la TSL publicada per l'òrgan competent de qualsevol país de la Unió Europea, d'acord amb el que estableix el ReIDAS.
- Els mecanismes emprats per a la identificació de persones físiques que autentiquin la identitat d'un ciutadà que declara representar una persona jurídica.

3.2. Sistemes de signatura

3.2.1. Persones físiques

S'admeten els sistemes de signatura següents, enumerats en l'annex 1 d'aquest document:

- Els certificats electrònics qualificats que hagin estat emesos per prestadors de serveis de certificació (PSC) inclosos en la TSL publicada per l'òrgan competent de qualsevol país de la Unió Europea, d'acord amb el que estableix el ReIDAS.
- Altres sistemes de signatura.

  Amb l'entrada en vigor de la Llei 39/2015, s'admeten també altres mecanismes d'identificació i signatura electrònica no criptogràfics basats en els mecanismes d'identificació electrònica, que s'emeten d'acord amb el que estableix l'article 10.2.c d'aquesta llei, més enllà dels certificats digitals, sempre que ho estableixi expressament la normativa reguladora aplicable.

3.2.2. Persones jurídiques i ens sense personalitat jurídica

S'admeten els sistemes de signatura següents, enumerats en l'annex 1 d'aquest document:

- Les persones jurídiques i els ens sense personalitat jurídica poden generar signatures electròniques amb els mecanismes d'identificació detallats en l'annex 1 d'aquest document.
- Els certificats de segell electrònic qualificat emesos a favor d'una persona jurídica o un ens sense personalitat per prestadors de serveis de certificació (PSC) inclosos en la TSL publicada per l'òrgan competent de qualsevol país de la Unió Europea, d'acord amb el que estableix el ReIDAS.
- Els mecanismes emprats per a la identificació de persones físiques que autentiquin la identitat d'un ciutadà que declara representar una persona jurídica.

3.3. Segells de temps

Les signatures electròniques en format avançat poden incorporar segells de temps generats per algun dels serveis següents:

- El servei de segell de temps que emet el Consorci Administració Oberta de Catalunya (AOC).
- Qualsevol altre servei de segell de temps qualificat d'acord amb el que estableix la secció 6 del ReIDAS i que hagi estat inclòs en una de les llistes de serveis de confiança publicades pels estats membres de la Unió Europea, d'acord amb el que estableix l'article 22 del ReIDAS.

3.4. Identificació i signatura dels representants

S'admeten els sistemes d'identificació i signatura següents, enumerats en l'annex 2 d'aquest document:

- Els certificats qualificats emesos a favor d'una persona jurídica o un ens sense personalitat jurídica (comunament anomenats també certificats electrònics de representant), amb indicació expressa de la representació que exerceix la persona física titular del certificat.
- Els certificats de segell electrònic qualificat emesos a favor d'una persona jurídica o un ens sense personalitat per prestadors de serveis de certificació (PSC) inclosos en la TSL publicada per l'òrgan competent de qualsevol país de la Unió Europea, d'acord amb el que estableix el ReIDAS.
- Els mecanismes emprats per a la identificació de persones físiques que autentiquin la identitat d'un ciutadà que representa una persona física, jurídica o una entitat sense personalitat jurídica. La representació s'ha d'acreditar per qualsevol mitjà vàlid en dret, inclosa la consulta en la plataforma de representació.
- El registre electrònic Representa del Consorci AOC o altres plataformes de representació habilitades.

4. Nivell de seguretat

D'acord amb el 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 al mercat interior (ReIDAS), els procediments han de dur associat un nivell de seguretat que sigui proporcional al grau de risc segons la confiança en la identitat de la persona que signa.

Per a definir el nivell de seguretat que s'ha d'aplicar, cal valorar els aspectes següents:

- La presència o no de dades de caràcter personal i el nivell de seguretat associat a aquestes dades.
- L'objecte, l'acte o el procediment sencer, la seva complexitat, les característiques de les dades que conté i la disposició documental dels documents associats.
- El grau de seguretat i garantia jurídica que requereixi l'acte o el procediment.

Els nivells de seguretat definits pel Reglament són: baix, substancial i alt.

El sistema d'identificació i el nivell de signatura requerits depenen, en primer lloc, del tipus de dades dins el context de cada procediment, del nivell de seguretat que el tràmit requereixi i del rol amb què actuï el titular del certificat (persona física, persona jurídica, etc.). En el catàleg de tràmits o en el document creat amb aquesta finalitat es detalla cada cas.

Per a cada nivell de seguretat només s'accepten uns determinats sistemes d'identificació i signatura. En l'annex 2 s'especifiquen els mecanismes d'identificació i signatura admesos per a cada nivell de seguretat.

4.1. Nivell de seguretat alt

Es requereix un nivell de seguretat alt en els sistemes d'identificació i signatura aplicables a:

a) Actes en què es doni accés o es transfereixin dades d'alt nivell de protecció segons l'article 9 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, o quan l'accés a les dades pugui afectar els drets de terceres persones especialment protegides per aquesta llei.

b) Els procediments de contractació, de conformitat amb la Llei 59/2003, de 19 de desembre, de signatura electrònica.

c) Tots aquells en què la normativa específica ho requereixi.

En aquests casos, els mecanismes d'identificació i signatura que s'han d'utilitzar són del tipus signatura electrònica basada en un certificat qualificat, segell de persona jurídica basat en un certificat qualificat o equivalents.

4.2. Nivell de seguretat substancial

Es requereix un nivell de seguretat substancial en els sistemes d'identificació i signatura aplicables, com a criteri general, als actes i serveis electrònics. Aquesta categoria inclou els formularis, les sol·licituds, la presentació de declaracions responsables, la interposició de recursos, el desistiment d'accions o la renúncia a drets.

En aquests casos, els mecanismes d'identificació i signatura que s'han d'utilitzar són del tipus signatura electrònica avançada, signatura electrònica basada en sistemes no criptogràfics o equivalents. Els mecanismes de signatura electrònica considerats admissibles per als tràmits classificats d'una categoria determinada són també admissibles per a les actuacions classificades de categoria inferior.

4.3. Nivell de seguretat baix

Es requereix l'establiment d'un nivell de seguretat baix en els sistemes d'identificació i signatura electrònica aplicables a:

a) Els actes electrònics o serveis electrònics d'un procediment administratiu, a excepció de tots aquells actes als quals s'aplica un nivell de seguretat substancial i que es relacionen més amunt.

b) Altres tràmits o procediments en què la normativa específica ho requereixi.

En aquests casos, els mecanismes d'identificació i signatura que s'han d'utilitzar són del tipus clau concertada o equivalents.

Addicionalment, els mecanismes de signatura electrònica considerats admissibles per als tràmits classificats d'una categoria determinada són també admissibles per a les actuacions classificades de categoria inferior.

4.4. Nivells de seguretat associats als procediments parlamentaris

Per a establir el nivell de seguretat associat als procediments parlamentaris i definir el risc que comporta la suplantació de la identitat i el no-repudi, s'ha tingut en compte, d'una banda, la naturalesa dels actes, i, de l'altra, l'entorn en què es desenvolupen.

Els **entorns** identificats són:

Tràmits en entorn tancat: els actes que presenten intercanvi de dades dins un entorn de seguretat habilitat a aquest efecte s'associen, en principi, a **un nivell baix o substancial**. Són els següents:

- Els actes fets pels diputats o els grups parlamentaris i el personal de la cambra, dins l'Administració parlamentària, amb relació a procediments parlamentaris o administratius.
- Els actes en què intervé una altra administració amb la qual s'ha establert un ambient de confiança mutu i s'han habilitat els mecanismes tecnològics que garanteixen la seguretat i la confidencialitat. En aquesta categoria es classifiquen els procediments en què interactuen el Parlament i el Govern de la Generalitat.

No obstant això, en funció de la **naturalesa dels actes**, es podria requerir un nivell de seguretat alt, com és el cas dels documents en què calgui garantir una validesa legal i una seguretat jurídica superior o bé quan la importància del document exigeix una protecció extra per a evitar fraus o disputes.

Tràmits en entorn obert: els actes que presenten intercanvi de dades entre el Parlament i qualsevol administració, organisme o ens del sector públic o privat, sense que hi hagi cap mecanisme tecnològic que garanteixi un entorn segur, s'associen, en principi, a un **nivell substancial**. Són els següents:

- Actes amb altres administracions: autonòmica (Síndic de Greuges, Sindicatura de Comptes, Oficina Antifrau de Catalunya, etc.), estatal (Senat, Congrés, ministeris, etc.), europea

(Parlament Europeu, Comissió Europea, Tribunal Europeu, etc.), local (ajuntaments, etc.), Administració de justícia, etc.

- Actes amb ens i organismes.
- Actes amb ciutadans.

5. Aprovació i manteniment de la Política d'identificació, signatura electrònica, segells electrònics i certificats

La Mesa del Parlament, a proposta del secretari general, aprova la Política d'identificació, signatura electrònica, segells electrònics i certificats, mitjançant l'acord corresponent, n'ordena la publicació al *Butlletí Oficial del Parlament*. Així mateix, se'n dona publicitat per mitjà del web del Parlament per a facilitar-ne el coneixement públic.

El secretari general, a proposta del Grup de Treball per a la Transformació Digital del Parlament de Catalunya, proposa a la Mesa del Parlament l'aprovació del següent:

- La modificació de la Política d'identificació, signatura electrònica, segells electrònics i certificats.
- Les normatives específiques que regulen, desenvolupen o milloren aspectes concrets amb relació a la Política d'identificació, signatura electrònica, segells electrònics i certificats.
- Les mesures necessàries per a dotar la institució dels recursos humans i materials necessaris per a desenvolupar una gestió eficaç i efectiva de la Política d'identificació, signatura electrònica, segells electrònics i certificats.

El Grup de Treball per a la Transformació Digital es responsabilitza de supervisar i validar les polítiques i altres normes específiques amb relació als sistemes d'identificació, signatura electrònica, segells electrònics i certificats, i també d'impulsar-ne l'aprovació o les modificacions posteriors.

5.1. Responsables que han de garantir l'aplicació de la Política d'identificació, signatura electrònica, segells electrònics i certificats

Els centres gestors que formen part del Grup de Treball per a la Transformació Digital del Parlament de Catalunya són els responsables de garantir el compliment de les directrius, les estratègies i els processos pel que fa als sistemes d'identificació, signatura electrònica, segells electrònics i certificats en els termes que estableix aquesta política.

El Departament de Gestió Documental i Recursos d'Informació i el Departament d'Informàtica i Telecomunicacions, en el marc d'aquesta política, tenen les responsabilitats següents:

- Elaborar la proposta de les modificacions de la Política d'identificació, signatura electrònica, segells electrònics i certificats.
- Elaborar la proposta de normes, protocols i instruccions que desenvolupin la Política d'identificació, signatura electrònica, segells electrònics i certificats.
- Formar i informar tots els usuaris del Parlament de Catalunya dels criteris i principis que conté aquesta política.

El Departament d'Informàtica i Telecomunicacions, com a responsable de l'entitat de registre del Parlament, té les responsabilitats següents:

- Gestionar les sol·licituds d'emissió i d'instal·lació de certificats i segells.
- Controlar el cicle de vida dels certificats i gestionar la documentació relativa als certificats.
- Gestionar tots els sistemes d'identificació.

Tots els centres gestors del Parlament, en el marc d'aquesta política, tenen les responsabilitats següents:

- Conèixer la Política d'identificació, signatura electrònica, segells electrònics i certificats.
- Complir les directrius que recull aquesta política.

6. Període de validesa

La Política d'identificació, signatura electrònica, segells electrònics i certificats entra en vigor en el termini d'un mes a comptar de la data de publicació en el Butlletí Oficial del Parlament.

7. Gestió i manteniment

La responsabilitat del manteniment i la gestió d'aquesta política correspon al Departament de Gestió Documental i Recursos d'Informació i al Departament d'Informàtica i Telecomunicacions com a part de les funcions del Grup de Treball per a la Transformació Digital.

Així mateix, s'estableix la publicació al web del Parlament d'aquesta política, del catàleg inicial i de les seves successives actualitzacions.

8. Normativa i referències

- 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 al mercat interior
- Decisió d'execució (UE) 2015/1506 de la Comissió, de 8 de setembre de 2015, per la qual s'estableixen les especificacions relatives als formats de signatures electròniques avançades i els segells avançats que han de reconèixer els organismes del sector públic, de conformitat amb els articles 27, apartat 5, i 37, apartat 5, del Reglament (UE) 910/2014
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals
- Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança
- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques
- Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic
- Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema nacional de seguretat
- Reial decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics
- Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema nacional d'interoperabilitat en l'àmbit de l'Administració electrònica
- Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança
- Codi del BOE d'Administració electrònica

Annex 1. Catàleg de sistemes d'identificació i signatura

El Parlament accepta els sistemes d'identificació i signatura següents:

A) Mecanismes no operats pel Parlament

	Tipus de credencial	Tipus de persona	Mecanisme	Operacions
M01	Certificat	Persona física	Certificats electrònics qualificats	Identificació i signatura
M02	Certificat	Persona jurídica	Segells electrònics qualificats	Identificació i signatura
M03	Certificat	Persona física representant de persona jurídica o ens sense personalitat jurídica	Certificats electrònics qualificats de representant	Identificació i signatura
M04	Sistema de claus concertades	Persona física	idCAT Mòbil	Identificació i signatura
M05	Sistema de claus concertades	Persona física	Cl@ve PIN	Identificació i signatura
M06	Sistema de claus concertades	Persona física	Cl@ve Permanente	Identificació i signatura
M07	Sistema de claus concertades	Persona física	Notificat a la Comissió Europea (capítol II ReIDAS)	Identificació

B) Mecanismes operats pel Parlament

	Tipus de credencial	Tipus de persona	Mecanisme	Operacions
M08	Sistema de claus concertades	Persona física	Usuari i contrasenya del Parlament	Identificació i signatura
M09	Sistema de claus concertades	Persona física	Usuari i contrasenya del Parlament amb 2FA	Identificació i signatura
M10	Sistema de claus concertades	Persona física	Evidència electrònica del Parlament	Signatura
M11	Sistema de claus concertades	Persona física	Evidència electrònica del Parlament amb 2FA	Signatura
M12	Certificat	Sistema informàtic	Certificat de servidor	Reconeixement

C) Descripció dels sistemes d'identificació i signatura

1) Certificats electrònics qualificats (M01)

   Certificat de signatura electrònica que ha estat emès a una persona física per un prestador de serveis de confiança qualificats d'acord amb el que estableix el ReIDAS.

   La Comissió Europea permet d'accedir a la llista completa de certificats qualificats de cada estat membre de la Unió en l'apartat «Trust Services» dins https://eidas.ec.europa.eu/efda/home.

2) Segells electrònics qualificats (M02)

   El Parlament de Catalunya s'ha d'identificar mitjançant un o diversos segells d'òrgan basats en un certificat digital reconegut d'acord amb la legislació vigent. Per als actes de signatura que no requereixin intervenció humana s'ha de fer servir un segell d'òrgan.

   La llista completa de certificats de segells electrònics qualificats es pot trobar als cercadors tant de la Comissió Europea com del ministeri competent en matèria d'autenticació i reconeixement de signatures electròniques.

3) Certificats electrònics qualificats de representant (M03)

   Són certificats per a persones físiques que demostren la seva condició de representant d'una persona jurídica o d'un ens sense personalitat jurídica.

4) Sistema de claus concertades (M04 a M06 i M08 a M11)

   Són mecanismes d'identificació electrònica no basats en l'ús de certificats electrònics i que empren com a factor d'autenticació el coneixement d'una clau prèviament acordada amb l'usuari. Per a augmentar-ne el nivell de seguretat, moltes vegades es combina aquest factor amb un altre de possessió, com ara tenir sota control un determinat dispositiu.

   El Parlament de Catalunya ha de proveir els diputats i el personal d'un codi d'usuari i una contrasenya. En el cas de la signatura sense certificat electrònic ha d'incloure els mecanismes adequats per a certificar l'expressió de voluntat de la persona signant i la integritat i la inalterabilitat de les dades signades.

5) Sistema d'identificació electrònica notificat a la Comissió Europea (M7)

   Sistema d'identificació electrònica notificat a la Comissió Europea d'acord amb el que defineix el capítol II del ReIDAS.

   Els ciutadans provinents d'un estat membre de la Unió Europea poden emprar un sistema d'identificació electrònica implantat al seu país d'origen si aquest ha estat notificat al node eIDAS, sempre que sigui compatible amb el sistema operatiu i hi estigui habilitat.

6) Certificat de servidor (M12)

   Un certificat de servidor permet la codificació o el xifratge de les dades trameses per tal que arribin al destinatari de forma segura, de manera que el destinatari és l'únic que pot descodificar-les, i per tant s'evita l'ús fraudulent de llocs webs o seus electròniques.

7) Evidència electrònica del Parlament (M10 i M11)

   Diferents mecanismes i tecnologies que permeten la traçabilitat de les accions i validar la integritat d'aquestes traces i documents.

   El codi segur de validació és un codi generat de manera automàtica que permet en tots els casos la comprovació de la integritat del document mitjançant l'accés a la seu electrònica corresponent.

   La funció resum (*hash*) d'una traça o document és un codi que permet de manera automàtica validar-ne la integritat i preservar-la de possibles alteracions.

D) Actualització dels sistemes d'identificació i signatura electrònica

El catàleg de sistemes d'identificació i signatura es pot actualitzar per a donar resposta a nous requisits funcionals o tècnics a proposta del Grup de Treball per a la Transformació Digital del Parlament de Catalunya i per mitjà de l'autorització del secretari general.

Annex 2. Mecanismes d'identificació i signatura per nivell de seguretat

Cada nivell de seguretat pot acceptar només uns determinats sistemes d'identificació i signatura. En aquest annex es determinen, per a cada nivell de seguretat, els mecanismes d'identificació i signatura admesos pel Parlament.

L'aplicació específica del mecanisme concret d'identificació i signatura s'ha de determinar seguint els criteris de seguretat, usabilitat i oportunitat tècnica, a partir dels mecanismes acceptats dins de cada nivell de seguretat, que són els següents:

A) Mecanismes d'identificació per nivell de seguretat

NS	Identificació	Intern (treballador del Parlament)	Extern (ciutadania, representant, treballador públic)	Integració de sistemes
NS1	Baix	M08 i M09	M01 a M09	
NS2	Substancial	M08 i M09	M01 a M06	M12
NS3	Alt	M09	M01 a M06	M12

B) Mecanismes de signatura per nivell de seguretat

NS	Identificació	Intern (treballador del Parlament)	Extern (ciutadania, representant, treballador públic)
NS4	Baix	M01 a M06 i M10 a M11	M01 a M06
NS5	Substancial	M01 a M06 i M11	M01 a M06
NS6	Alt	M01 a M03	M01 a M03

C) Actualització de la relació entre els nivells de seguretat i els mecanismes d'identificació

Els mecanismes d'identificació i signatura per nivell de seguretat es poden actualitzar per a donar resposta a nous requisits funcionals o tècnics a proposta del Grup de Treball per a la Transformació Digital del Parlament de Catalunya i per mitjà de l'autorització del secretari general.

Annex 3. Glossari

Autenticació: procés de verificació de la identitat digital d'un subjecte en les seves interaccions en l'àmbit digital. L'autenticació requereix factors com certificats, contrasenyes, claus concertades o elements biomètrics.

Certificat electrònic: document digital emès per un proveïdor de serveis de confiança (autoritat de certificació) que identifica una clau pública amb el seu propietari. Serveix per a garantir la identificació i la signatura del titular. Els certificats tenen un número de sèrie únic i un període de validesa o caducitat que s'inclou en el mateix certificat.

Document: tota informació, amb caràcter únic i en qualsevol suport o format, que és evidència d'accions, decisions i funcions pròpies de les persones físiques i jurídiques, incloent les bases de dades i altres objectes electrònics de qualsevol naturalesa.

Document electrònic: document en què la informació és manipulada, transmesa o processada per mitjans informàtics i té contingut, context i estructura suficients per a testimoniar l'activitat que l'ha generat.

Identificació: procediment per a reconèixer de manera única un subjecte que requereix un registre previ amb l'assignació d'un element identificador que permeti la identificació única de la persona física o jurídica.

Segell de temps: assignació per mitjans electrònics d'una data i hora a un document electrònic amb la intervenció d'un prestador de serveis de certificació que acrediti l'exactitud i integritat de la marca de temps del document.

Segell electrònic: conjunt de dades associades a un document que permeten d'assegurar la identitat del signant i la integritat del contingut. En aquest cas, el signant és una persona jurídica i la forma és un segell.

Signatura electrònica: dades en format electrònic, consignades o associades a altres dades de manera lògica, que utilitza el signant per a signar. Conjunt d'elements que intervenen en la creació de la signatura electrònica.

Signatura digital: conjunt de dades associades a un document que permeten d'assegurar la identitat del signant i la integritat del contingut. El signant genera una funció resum del contingut o missatge, que xifra amb la seva clau privada i dona com a resultat la signatura digital. Aquesta permet de comprovar l'autoria amb la clau pública del signant.