Administració Oberta de Catalunya

Localret

# Protocol d'identificació i signatura electrònica de Catalunya

Generalitat de Catalunya

Localret

Administració Oberta de Catalunya

Localret

# Control documental

| | |
|---|---|
| **Estat formal** | |
| **Elaborat per** | Consorci AOC |
| **Aprovat per** | |
| **Data de creació** | 01/12/2024 |
| **Nivell accés informació** | Pública |
| **Títol** | Protocol d'identificació i signatura electrònica de Catalunya |
| **Fitxer** | Protocol d'identificació i signatura electrònica de Catalunya 2024.dotx |
| **Control de còpies** | Només les còpies disponibles a la Seu electrònica del Consorci AOC garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades. |
| **Drets d'autor** |  |

# Control de versions

| | |
|---|---|
| **Data:** | 1/12/2024 |
| **Descripció:** | Primera versió |

# Índex

**1. Introducció ..... 4**

**2. Objecte de la guia ..... 5**

**3. Nivells de seguretat dels sistemes ..... 6**

**3.1. Identificació i autenticació ..... 6**

**3.2. Signatura electrònica i segells electrònics ..... 6**

**4. Catàleg de mecanismes ..... 7**

**4.1. Mecanismes d'identificació ..... 7**

4.1.1. Per a ciutadans ..... 7
4.1.2. Per empreses ..... 8
4.1.3. Per als empleats públics ..... 8
4.1.4. Pels ens de l'administració davant dels ciutadans: ..... 9
4.1.5. Cartera europea d'identitat digital ..... 9

**4.2. Mecanismes de signatura i segell electrònic ..... 9**

4.2.1. Per a ciutadans ..... 9
4.2.2. Per empreses ..... 10
4.2.3. Per als empleats públics: ..... 10
4.2.4. Pels ens de l'Administració davant dels ciutadans: ..... 10
4.2.5. Segells de temps ..... 10

**5. Interoperabilitat de les signatures electròniques ..... 11**

**5.1. Interoperabilitat de signatures electròniques no basades en certificats qualificats ..... 11**

**5.2. Polítiques de signatura ..... 11**

**6. Admissió de mecanismes d'identificació i de signatura electròniques .. 11**

**6.1. Admissió de mecanismes d'identificació electrònica ..... 11**

6.1.1. Per als tràmits classificats de categoria Alta ..... 12
6.1.2. Per als tràmits classificats de categoria Mitjana o substancial ..... 12
6.1.3. Per als tràmits classificats de categoria Baixa ..... 13

**6.2. Admissió de mecanismes de signatura electrònica ..... 13**

6.2.1. Per als tràmits classificats de categoria Alta ..... 13
6.2.2. Per als tràmits classificats de categoria Substancial ..... 14
6.2.3. Per als tràmits classificats de categoria Baixa ..... 14

**6.3. Ús de segells de temps ..... 14**

**7. Criteris d'aplicació ..... 15**

**8. El Consorci AOC i els mecanismes de identificació i signatura ..... 16**

# 1. Introducció

El 23 de juliol de 2014 el Parlament Europeu i el Consell de la Unió Europea van aprovar el Reglament Nº 910/2014 relatiu a la identificació electrònica i els serveis de confiança per les transaccions electròniques en el mercat interior, conegut com a ReIDAS, estableix, d'acord al que especifica el seu article 1, el marc jurídic per les signatures electròniques, segells electrònics, segells de temps, documents electrònics i serveis d'entrega electrònica certificada i els serveis certificats d'autenticació web, així com les condicions en que s'han d'admetre els sistemes d'identificació electrònica de persones físiques i jurídiques que donen servei en d'altres Estats membre. Sobre aquests, ReIDAS descrivia un esquema de tres nivells de seguretat per als mecanismes d'identificació, que van queda definits al Reglament d'Execució de la Comissió Europea 2015/1502 de 8 de Setembre de 2015.

Els prestadors de serveis de confiança establerts a l'estat espanyol han de complir addicionalment amb el que estableix la Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança. Pel que fa a les administracions públiques, la Llei 39/2015 de Procediment Administratiu Comú de les Administracions Públiques, en el seu Títol I, Capítol II, estableix, amb caràcter bàsic, un conjunt mínim de categories de mecanismes d'identificació i signatura electrònica a acceptar per part de les Administracions, coherent i complementari al especificat a ReIDAS. Aquesta llei, als articles 9 i 10, deixa en mans de cada Administració el determinar l'admissió de sistemes d'identificació i signatura a l'hora de portar a terme determinats tràmits o procediments, tot i que l'admissió dels sistemes basats en certificats digitals continua sent obligatòria.

Per altra banda, La Llei 40/2015, d1 d'octubre, de Règim jurídic del Sector Públic, al seu Capítol V i el Real Decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics al seu capítol II són els que regulen els mecanismes d'identificació i signatura electrònica que empren les administracions públiques i el seu personal en la seva actuació telemàtica.

Amb l'objectiu d'orientar a les administracions a l'hora de seleccionar els mecanismes d'identificació i signatura electrònica que resulten admissibles per una actuació concreta d'entre els que compleixen amb els requisits jurídicament establerts per la normativa descrita, l'Esquema Nacional de Seguretat, aprovat pel Reial Decret 311/2022, de 3 de maig (en endavant, ENS) preveu que els mecanismes d'identificació i signatura electrònica poden tenir tres nivells de seguretat, i estableix els criteris per a la seva admissió i ús. També estableix els criteris per determinar quin nivell requereix un sistema o una actuació concreta.

Per tal de garantir la interoperabilitat dels documents signats electrònicament, el Real Decret 4/2010, de 8 de gener, que regula l'Esquema Nacional d'Interoperabilitat, al seu Capítol IX estableix un conjunt de requisits relatius a les polítiques de signatura electrònica i conservació de documents que les administracions també caldrà que tinguin en consideració.

En l'àmbit de Catalunya, van aprovar-se la Llei 29/2010, de 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya i la Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya, completen el cos normatiu dedicat a l'ús dels mitjans electrònics a Catalunya i són aplicables a totes les administracions catalanes.

En aquest sentit, el Decret 76/2020, de 4 d'agost, d'Administració digital, l'Ordre VPD/93/2022, de 28 d'abril, per la qual s'aprova el Catàleg de sistemes d'identificació i signatura electrònica i l'Ordre PRE/158/2022, de 30 de juny, per la qual s'aprova la Guia d'ús dels sistemes d'identificació i signatura electrònica en l'àmbit de l'Administració de la Generalitat, desenvolupen -en l'àmbit de l'Administració de la Generalitat de Catalunya- les disposicions en matèria d'identificació i signatura electrònica. D'aquesta manera, determinen els mecanismes admesos i estableixen quins d'ells poden utilitzar la ciutadania i les empreses en les serves relacions amb l'Administració de la Generalitat.

Pel que fa al Consorci Administració Oberta de Catalunya, la esmentada Llei 29/2010, en el seu article 7.3, estableix que, en el marc de les competències que li atribueixen els seus estatuts o que li deleguen les administracions públiques que en formen part, una de les funcions que exerceix és la d'elaborar criteris i recomanacions per garantir la interoperabilitat de la informació derivada de l'actuació de les entitats que conformen el sector públic de Catalunya. També actua com a Proveïdor de Serveis de Certificació, identificació i signatura electrònica.

Finalment, l'any 2024 el Parlament Europeu va aprovar el Reglament (UE) 2024/1183 del Parlament Europeu i del Consell, d'11 d'abril del 2024, pel qual es modifica el ReIDAS pel que fa a l'establiment del marc europeu d'identitat digital, introduint un nou model basat en les anomenades carteres d'identitat digital, i ampliant el número de serveis de confiança contemplats a la normativa amb l'objectiu de millorar la seva implantació i ús transfronterer, superant les limitacions de l'anterior model.

# 2. Objecte de la guia

El marc jurídic descrit, i més tenint en compte els canvis que s'han anat produint des de l'any 2010, deixa en bona part en mans de cada administració la decisió sobre quins mecanismes d'identificació i signatura electrònica s'han d'acceptar per cada tipus d'actuació, sempre que les normes que la regulen així ho permetin.

L'objecte d'aquesta guia és la de oferir un conjunt de criteris comuns tècnics i organitzatius per la implantació dels sistemes de identificació i signatura electrònica per a cada tràmit o servei, tenint en compte el seu nivell de seguretat i donant compliment als requisits establerts per la normativa jurídica.

# 3. Nivells de seguretat dels sistemes

En aquest apartat es defineix la classificació dels diferents tipus de sistemes de identificació i signatura electrònica d'acord amb la normativa aplicable.

## 3.1. Identificació i autenticació

El ReIdAS, anomena "identificació electrònica" al procés d'emprar les dades d'identificació d'una persona en format electrònic que representen de manera única a una persona física o jurídica, o bé a una persona física que representa a una persona física. El procés electrònic que possibilita aquesta identificació, o de l'origen i integritat d'unes dades rep el nom "d'autenticació".

El Reglament tracta de manera separada els sistemes de identificació electrònica, que possibiliten aquests processos, de la resta de serveis de confiança, i estableix (a l'article 8) tres nivells de seguretat:

- Nivell de seguretat baix, amb l'objectiu de reduir el risc d'ús indegut o alteració de la identitat presentada.
- Nivell de seguretat substancial, amb l'objectiu de reduir substancialment el risc d'ús indegut o alteració de la identitat.
- Nivell de seguretat alt, amb l'objectiu d'evitar l'ús indegut o alteració de la identitat.

El nivell de seguretat assolit per un sistema de identificació electrònica es determina d'acord al que estableix el Reglament d'Execució de la Comissió Europea 2015/1502 de 8 de Setembre de 2015, i és aquest criteri el que empra aquesta guia a l'hora de classificar-los.

## 3.2. Signatura electrònica i segells electrònics

Tenint en compte la seva la definició descrita a l'article 3 de ReIDAS, la tipologia de mecanismes de signatura i segell electrònic és la següent:

- Signatures i segells electrònics
- Signatures i segells electrònics avançats
- Signatures i segells electrònics avançats basats en certificats qualificats
- Signatures i segells electrònics qualificats

Tal i com els defineix el propi ReIDAS (article 3), la signatura electrònica són les dades en format electrònic annexades a altres dades o associades amb aquestes de manera lògica que empra el signatari per signar, mentre que el segell electrònic és un mecanisme que garanteix l'origen i la integritat d'unes dades. Qualsevol mecanisme que encaixi amb aquestes definicions quedaria doncs classificat dintre de la primera categoria.

La segona categoria seria per mecanismes de segell i signatura electrònica “avançats”, que d’acord amb el que estableixen els articles 26 i 36, haurien de complir amb els següents requisits:

- Estar vinculats al signatari o al creador del segell de manera única
- Permetre la identificació del signatari o creador del segell
- Haver estat creat emprant dades que el signatari o creador del segell pugui emprar, amb un alt nivell de confiança, sota el seu control exclusiu
- Garantir la integritat de les dades signades o segellades

La tercera seria la de les signatures i segells generats emprant certificats digitals emesos per un Prestador de Serveis de Certificació qualificat, mentre que la quarta seria la de les signatures i segells generats emprant dispositius segurs de creació de signatura i segell. Aquesta darrera categoria seria la equiparable a la signatura manuscrita amb validesa legal a tots els països de la Unió Europea.

# 4. Catàleg de mecanismes

A continuació es descriuen els mecanismes de identificació i signatura disponibles en l’actualitat tenint en compte el seu subjecte i funció.

## 4.1. Mecanismes d'identificació

### 4.1.1. Per a ciutadania

- Els certificats electrònics qualificats que hagin estat emesos per Prestadors de Serveis de Certificació (PSCs) inclosos a la Llista de confiança de Prestadors de Serveis de Certificació (TSL, per les sigles en anglès Trusted Services List) publicada per l’òrgan competent de qualsevol país de la Unió Europea d’acord amb el que estableix ReIDAS.
- S’hauran d’admetre, amb caràcter general, qualsevol dels mitjans d'identificació inclosos a la llista que publica la Comissió Europea, per accedir als serveis prestats en línia per un organisme del sector públic en un Estat Membre, a efectes de l'autenticació transfronterera, conforme al que estableix el mateix reglament.
- El certificat qualificat reconegut de signatura avançada idCAT per a ciutadania que emet el Consorci AOC.
- El mecanisme idCAT Mòbil que és un mecanisme d'identificació i signatura electrònica dels ciutadans (persones físiques) no criptogràfic basat en l’enviament de paraules de pas codis d’un sol us a dispositius mòbils, operat pel Consorci AOC.

- idCAT Mòbil +, com a modalitat de l'anterior que garanteix un nivell de seguretat superior amb doble factor d'autenticació i registre amb seguretat equiparable al presencial.
- La cartera europea d'identitat digital de les persones interessades que resideixen a altres Estats de la Unió Europea, conforme el que disposa l'article 5 septies.1 del ReIDAS.

### 4.1.2. Per empreses

- Els certificats qualificats emesos a una persona física amb indicació expressa de la representació que ostenta sobre una persona jurídica o un ens sense personalitat jurídica.
- Els certificats de segell electrònic qualificat emesos a una persona jurídica o a un ens sense personalitat per PSCs inclosos a la TSL publicada per l'òrgan competent de qualsevol país de la Unió Europea d'acord amb el que estableix el ReIDAS.
- També els mecanismes indicats per a la identificació de persones físiques, quan s'emprin per autenticar la identitat d'un ciutadà que declara representar a una persona jurídica. Quan s'escaigui, aquesta representació es podrà verificar mitjançant la consulta a un registre en línia de representacions; especialment, mitjançant el servei REPRESENTA del Consorci AOC, les condicions del qual es publiquen a la seva web.
- La cartera europea d'identitat digital de les persones interessades que resideixen a altres Estats de la Unió Europea, conforme el que disposa l'article 5 septies.1 del ReIDAS.

### 4.1.3. Per als empleats públics

- El certificat electrònics qualificats que el Consorci AOC emet al empleats del Sector Públic de Catalunya en dispositiu segur de creació de signatura: la T-CAT.
- El certificat electrònic qualificat que el Consorci AOC emet al empleats del Sector Públic de Catalunya en suport programari: la T-CAT P.
- Els certificats electrònics qualificats emesos per prestadors inclosos a la TSL publicada pel Ministeri per a la Transformació Digital i funció pública (o organisme competent) conforme al perfil "Empleado público" aprovat pel Consejo Superior de Administración Electrónica.
- D'altres sistemes no criptogràfics, com els usuaris i contrasenyes que alguns ens del Sector Públic de Catalunya emeten al personal al seu càrrec, o els que s'utilitza com a mecanisme d'identificació la plataforma EACAT.
- Qualsevol perfil de certificats reconeguts o qualificats emesos per prestadors inclosos a la TSL publicada pel Ministeri corresponent que acreditin la vinculació del seu titular a un ens públic.

### 4.1.4. Pels ens de l'administració davant dels ciutadans:

- Els certificats electrònics qualificats emesos pels PSCs inclosos a la TSL del Ministeri corresponent conforme al perfil "Sede electrónica administrativa" aprovat pel Consejo Superior de Administración Electrónica.
- D'altres certificats qualificats d'autenticació de lloc web, d'acord al que estableix l'Article 45 de ReIDAS, emesos a nom d'un ens.

### 4.1.5. Cartera europea d'identitat digital

D'acord a la definició que en fa l'article 3 del ReIDAS, modificat pel Reglament (UE) 2024/1183 del Parlament Europeu i del Consell, d'11 d'abril de 2024, respecte a l'establiment del marc europeu d'identitat digital, una cartera europea d'identitat digital és un mitjà d'identificació electrònica que permet a l'usuari emmagatzemar, gestionar i validar de manera segura dades d'identificació de la persona i declaracions electròniques d'atributs per tal de proporcionar-los a les parts usuàries i altres usuaris de carteres europees d'identitat digital, així com signar per mitjà de signatures electròniques qualificades o segellar per mitjà de segells electrònics qualificats.

En compliment de l'article 5 septies del mateix Reglament, els organismes del sector públic hauran d'acceptar les carteres europees d'identitat digital sempre quan exigeixin una identificació i autenticació electrònica. L'ús dels serveis comuns d'identificació electrònica que el Consorci AOC ofereix al conjunt de les Administracions Públiques Catalanes facilitarà tecnològicament el compliment d'aquest requisit.

## 4.2. Mecanismes de signatura i segell electrònic

Amb caràcter general, els mecanismes de signatura establerts en aquest apartat, tenen així mateix, efectes d'identificació del ciutadans i ciutadanes i d'empleat públics.

### 4.2.1. Per a ciutadans

- Els certificats electrònics qualificats que hagin estat emesos per PSCs inclosos a la TSL publicada per l'òrgan competent de qualsevol país de la Unió Europea d'acord amb el que estableix el ReIDAS.
- El certificat reconegut o qualificat de signatura avançada idCAT que emet el Consorci AOC.
- S'hauran d'admetre els certificats del DNI-e, d'acord al que estableix la disposició addicional tercera de la Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.

- El mecanisme no criptogràfic de signatura ordinària que el sistema VALID del Consorci AOC ofereix a les aplicacions de les Administracions Públiques Catalanes i ens del sector públic que s'hi integren.

### 4.2.2. Per empreses

Les persones jurídiques i els ens sense personalitat jurídica podran emprar signatures electròniques els mecanismes d'identificació llistats al punt 4.1.2 d'aquest protocol.

### 4.2.3. Per als empleats públics:

Els empleats públics podran emprar per produir signatures electròniques els mecanismes d'identificació llistats al punt 4.1.3 d'aquest protocol.

### 4.2.4. Pels ens de l'Administració davant dels ciutadans:

- Els certificats qualificats de segell electrònic que el Consorci AOC emet als ens del Sector Públic de Catalunya.
- Els certificats electrònics qualificats emesos per altres PSCs inclosos a la TSL del Ministeri corresponent conforme al perfil "Sello electrónico" aprovat pel Consejo Superior de Administración Electrónica.
- En l'àmbit de l'actuació administrativa automatitzada, d'acord al que disposa la Llei 40/2015, de l'1 d'octubre:
    - El codi segur de verificació (CSV), com a mecanisme de signatura electrònica dels ens i dels seus empleats públics davant dels ciutadans, vinculat a un ens, òrgan i, si és cas, a la persona signatària del document; el qual permet comprovar la integritat del document així signat mitjançant la consulta de l'original a la seu electrònica corresponent per fer-ne l'acarament..
    - Els certificats electrònics qualificats de segell electrònic que el Consorci AOC emet als ens del Sector Públic de Catalunya.

Es recomana que, quan en l'àmbit de l'actuació administrativa automatitzada es generin signatures mitjançant un codi segur de verificació (CSV), els documents també se signin amb un certificat de segell electrònic per garantir-ne la integritat.

### 4.2.5. Segells de temps

Les signatures electròniques avançades podran incorporar segells de temps generats per algun dels següents serveis:

- El servei Segell de temps del Consorci AOC;

- Qualsevol altre servei de segell de temps qualificat conforme al que estableix la Secció 6 de ReIDAS i que hagi estat inclòs a una de les llistes de serveis confiança publicades pels Estats Membres de la Unió Europea, segons estableix l'Article 22 del mateix Reglament.

# 5. Interoperabilitat de les signatures electròniques

## 5.1. Interoperabilitat de signatures electròniques no basades en certificats qualificats

Tal i com estableix l'article 45 de la Llei 40/2015, de l'1 d'octubre, quan una Administració empri sistemes de signatura electrònica no basats en certificats electrònics reconeguts o qualificats, a l'hora d'enviar els documents signats a d'altres administracions, podrà superposar un segell electrònic basat en un certificat per tal de donar garanties sobre la seva validesa.

## 5.2. Polítiques de signatura

Emprant certificats qualificats tant d'empleat públic com de segell electrònic, acceptant certificats qualificats de persona física per part de la ciutadania i emprant els serveis comuns de validació i signatura electrònica que l'AOC ofereix amb acord al que estableix aquest Protocol, les Administracions Públiques catalanes estan complint amb els requisits establerts per la Política de Signatura Electrònica de l'Administració General de l'Estat conforme al que estableix l'article 18 de l'ENS.

# 6. Admissió de mecanismes d'identificació i de signatura electròniques

## 6.1. Admissió de mecanismes d'identificació electrònica

L'admissió del mecanismes d'identificació i signatura electrònica es realitza conforme als nivells de seguretat requerits a l'Annex del Reglament d'Execució 2015/1502 de la Comissió Europea i a l'ENS en relació amb la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets digitals.

Els mecanismes d'identificació electrònica considerats admissibles per als tràmits d'una categoria determinada, són també admissibles per als tràmits classificats de categoria inferior a aquesta.

Quan en el context d'un servei electrònic calgui garantir la protecció de la confidencialitat de les dades implicades mitjançant mecanismes d'identificació electrònica, s'admetran els següents.

### 6.1.1. Per als tràmits classificats de categoria Alta

S'admeten els sistemes d'identificació electrònica de nivell de seguretat alt, com aquells que fan un registre dels usuaris presencial i fiable i proveeixen els usuaris d'un mitjà d'identificació electrònica de doble factor.

S'admeten amb caràcter obligatori:

- Aquells certificats electrònics qualificats, que s'emetin en un dispositiu qualificat de creació de signatura electrònica, entre els establerts en el punt 4 d'aquest document, atenent a les tipologies de certificats i del col·lectiu específic.
- Qualsevol dels mitjans d'identificació que hagi estat notificat de nivell de seguretat alt i s'inclogui a la llista que - conforme al que estableix el ReIDAS al capítol 2 - publicarà la Comissió Europea per accedir als serveis prestats en línia per un organisme del sector públic en un Estat Membre, a efectes de l'autenticació transfronterera.
- Les carteres d'identitat digital europees amb acord al que estableix l'article 6 bis del ReIDAS.

### 6.1.2. Per als tràmits classificats de categoria Mitjana o substancial

S'admeten els sistemes d'identificació electrònica de nivell de seguretat mitjana o substancial, com aquells que fan un registre fiable dels usuaris, el qual es podrà dur a terme de manera presencial o remota (on-line) i proveeixen els usuaris d'unes credencials de robustesa substancial.

Concretament:

- Obligatòriament, els certificats electrònics qualificats i els certificats electrònics qualificats de segell electrònic establerts en el punt 4. d'aquest document, atenent a les tipologies de certificats i del col•lectiu específic.
- Obligatòriament, qualsevol dels mitjans d'identificació que hagi estat notificat de nivell de seguretat substancial i s'inclogui a la llista que - conforme al que estableix el ReIDAS al capítol 2 - publica la Comissió Europea per accedir als serveis prestats en línia per un organisme del sector públic en un Estat Membre, a efectes de l'autenticació transfronterera.
- El mecanisme idCAT Mòbil + amb doble factor d'autenticació.
- Qualsevol altre mecanisme integrat al servei VAlid operat pel Consorci AOC i classificat com a de nivell mig d'acord amb les especificacions marcades per l'ENS i del Reglament d'Execució 2015/1502 de la Comissió Europea.

### 6.1.3. Per als tràmits classificats de categoria Baixa

Seran admissibles els mecanismes d'identificació amb acord al que estableix el punt 4.2.5 de l'Annex II de l'ENS. En concret es podrà admetre idCAT Mòbil en totes les seves modalitats, així com la resta de mecanismes descrits en aquest document.

## 6.2. Admissió de mecanismes de signatura electrònica

Amb caràcter general, les persones físiques interessades poden acreditar mitjançant una signatura electrònica l'autenticitat de l'expressió de la seva voluntat i consentiment, així com la integritat i la inalterabilitat de les dades i/o documents a signar.

Una persona jurídica o un ens sense personalitat pot acreditar l'origen i la integritat de les dades i/o dels documents que remeti en el context d'un servei electrònic, mitjançant un segell electrònic o una signatura electrònica qualificada del representant de l'ens.

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 a aquesta.

En particular, quan en el context d'un servei electrònic es requereixi una signatura electrònica s'admetran les següents.

### 6.2.1. Per als tràmits classificats de categoria Alta

S'admeten signatures electròniques qualificades o segells electrònics qualificats, segons correspongui, i amb caràcter obligatori:

- Quan als formats: els serveis electrònics oferts pels organismes dels Estats Membres de la Unió Europea han de reconèixer les signatures qualificades que siguin conformes a algun dels formats de referència que determina la Decisió d'Execució (UE) 2015/1506 de la Comissió, de 8 de setembre, per la que s'estableixen les especificacions relatives als formes de signatura avançada i els segells avançats que han de reconèixer els organismes del sector públic de conformitat amb l'article 27, apartat 5, i 37, apartat 5, del ReIDAS.
- Pel que fa als certificats emprats: s'han d'admetre les signatures electròniques generades amb aquells certificats electrònics qualificats de signatura electrònica, entre els considerats a l'apartat 6.2 d'aquest document, que s'emetin en un dispositiu qualificat de

creació de signatura electrònica. També els segells electrònics generats amb aquells certificats de segell electrònic qualificat, entre els considerats a l'apartat 6.2, que s'emetin en un dispositiu qualificat de creació de segells electrònics, tenint en compte la tipologia descrita.

### 6.2.2. Per als tràmits classificats de categoria Substancial

Seran admissibles les signatures electròniques avançades basades en un certificat qualificat de signatura electrònica i els segells electrònics avançats basats en certificats qualificats de segell electrònic, així com les signatures electròniques ordinàries generades a partir d'un mecanisme d'identificació de nivell de seguretat substancial – com els considerats a l'apartat 4.1.2 d'aquest document.

Concretament:

- S'hauran de reconèixer les signatures electròniques avançades i les signatures avançades basades en un certificat qualificat de signatura electrònica que siguin conformes a algun dels formats de referència definits al Reglament d'Execució 2015/1506 de la Comissió Europea, o que s'hagin generat amb els mètodes de referència - quan siguin d'un format alternatiu; segons el que estableix a l'article 27 del ReIDAS, a efectes de garantir el correcte tractament dels documents signats electrònicament.
- Pel que fa als certificats emprats: s'haurien d'admetre les signatures electròniques generades amb els certificats de signatura electrònica considerats a l'apartat 4.2 d'aquest document. També els segells electrònics generats amb els certificats de segell electrònic considerats al mateix apartat 4.2, atenen a les tipologies de certificats que es llisten per a cadascun dels col·lectius que es distingeixen.
- Seran admissibles les signatures ordinàries basades en el mecanisme idCAT Mòbil + amb doble factor d'autenticació.
- També les signatures ordinàries basades en altre mecanismes que hagin estat classificat de nivell mig o substancial integrats  al servei VAlid operat pel Consorci AOC.

### 6.2.3. Per als tràmits classificats de categoria Baixa

S'admeten els mecanismes que generen signatures electròniques ordinàries prenent com a fonament un mecanismes d'identificació com els descrits a l'apartat 5.1.3.

## 6.3. Ús de segells de temps

S'admeten les signatures electròniques avançades que incorporen segells de temps generats per algun dels serveis descrits a l'apartat 4.2.5.

# 7. Criteris d'aplicació

Amb caràcter general, s'admetran tots els mecanismes d'identificació i signatura electrònica exposats en aquest protocol per a tots els tràmits i serveis. Cada organisme podrà excloure l'admissió dels mecanismes de nivell baix i, si s'escau, substancial per l'existència de:

- Risc jurídic: pel que fa a un procediment concret, valoració de l'existència d'un risc que impedeix garantir la viabilitat i seguretat jurídica del procediment amb motiu d'un possible frau en la signatura del document o de la suplantació d'identitat de les persones interessades, que tingui com a origen la manca de robustesa dels sistemes d'identificació o de signatura electrònica.
- Risc de Ciberseguretat o protecció de dades: valoració de la necessitat de mesures específiques més restrictives que es determinin en funció del nivell de risc o classificació de la informació, del servei o tràmit o del possible tractament de dades personals derivats del tràmit o servei respecte al qual es prevegi utilitzar el sistema d'identificació o de signatura electrònica.

En aquest sentit, caldrà tenir en consideració el criteri establert per l'Annex I, punt 3, de l'Esquema Nacional de Seguretat que requereix l'aplicació dels tres nivells considerats en aquest protocol segons el següent criteri:

**Nivell BAIX**. S'aplicarà quan les conseqüències d'un incident de seguretat que afecti alguna de les dimensions de seguretat suposin un perjudici limitat sobre les funcions de l'organització, els actius o els individus afectats.

S'entendrà per perjudici limitat:

1. La reducció de manera apreciable de la capacitat de l'organització per desenvolupar eficaçment les seves funcions i competències, encara que aquestes es continuïn exercint.
2. Causar un dany menor als actius de l'organització.
3. L'incompliment formal d'alguna llei o regulació, que tingui caràcter d'esmenable.
4. Causar un perjudici menor a algun individu, que malgrat resultar molest, pugui ser fàcilment reparable.
5. Altres de naturalesa anàloga.

**Nivell MITJÀ.** S'aplicarà quan les conseqüències d'un incident de seguretat que afecti alguna de les dimensions de seguretat suposin un perjudici greu sobre les funcions de l'organització, els actius o els individus afectats.

S'entendrà per perjudici greu:

1. La reducció significativa de la capacitat de l'organització per desenvolupar eficaçment les seves funcions i competències, encara que aquestes es continuïn exercint.
2. Causar un dany significatiu als actius de l'organització.
3. L'incompliment material d'alguna llei o regulació, o l'incompliment formal que no tingui caràcter d'esmenable.

4. Causar un perjudici significatiu a algun individu, de reparació difícil.
5. Altres de naturalesa anàloga.

**Nivell ALT.** S'aplicarà quan les conseqüències d'un incident de seguretat que afecti alguna de les dimensions de seguretat suposin un perjudici molt greu sobre les funcions de l'organització, els actius o els individus afectats.

S'entendrà per perjudici molt greu:

1. L'anul·lació efectiva de la capacitat de l'organització per desenvolupar eficaçment les funcions i les competències.
2. Causar un dany molt greu i fins i tot irreparable dels actius de l'organització.
3. L'incompliment greu d'alguna llei o regulació.
4. Causar un perjudici greu a algun individu, de reparació difícil o impossible.
5. Altres de naturalesa anàloga.

# 8. El Consorci AOC i els mecanismes de identificació i signatura

El Consorci AOC ofereix al conjunt de les Administracions Públiques Catalanes dos serveis que permeten garantir el nivell de seguretat dels sistemes d'identificació i signatura emprats. Aquests són:

- Servei Validador, que permet validar les signatures electròniques basades en certificats qualificats o reconeguts, i que informa del nivell de seguretat assolit per aquestes depenent del perfil del certificat emprat.
- Servei VAlid, que permet emprar sistemes d'identificació dels tres nivells de seguretat.

Ambdós serveis informen del nivell de seguretat assolit en els processos d'identificació i signatura electrònica que ofereixen o donen suport. Al lloc web del Consorci AOC es poden trobar els documents de classificació que el Consorci AOC manté, i que llisten els mecanismes que els dos serveis suporten amb el nivell de seguretat que ofereixen.

L'aplicació dels criteris que es descriuen en aquesta guia es pot basar en aquestes classificacions que el Consorci AOC porta a terme en base a la normativa actual que hem descrit en aquesta guia.