



**Consorci
Administració Oberta
de Catalunya**

Protocol d'Identificació i Signatura Electrònica de Catalunya

 **Generalitat
de Catalunya**

LOCALRET

Índex

1	Introducció	1
2	Objecte de la guia	1
3	Nivells de seguretat dels sistemes	2
3.1	Identificació i autenticació	2
3.2	Signatura electrònica i segells electrònics.....	2
4	Catàleg de mecanismes	3
4.1	Mecanismes d'identificació	3
4.1.1	Per a ciutadans	3
4.1.2	Per empreses	3
4.1.3	Per als empleats públics	4
4.1.4	Pels ens de l'administració davant dels ciutadans:.....	4
4.2	Mecanismes de signatura i segell electrònic.....	4
4.2.1	Per a ciutadans	4
4.2.2	Per empreses	5
4.2.3	Per als empleats públics:	5
4.2.4	Pels ens de l'Administració davant dels ciutadans:	5
4.2.5	Segells de temps	5
4.2.6	Interoperabilitat de les signatures electròniques.....	6
5	Admissió de mecanismes d'identificació i de signatura electròniques.....	6
5.1	Admissió de mecanismes d'identificació electrònica	6
5.1.1	Per als tràmits classificats de categoria Alta:.....	6
5.1.2	Per als tràmits classificats de categoria Mitjana o substancial:.....	7
5.1.3	Per als tràmits classificats de categoria Baixa	7
5.2	Admissió de mecanismes de signatura electrònica.....	7
5.2.1	Per als tràmits classificats de categoria Alta.....	7

5.2.2	Per als tràmits classificats de categoria Substancial.....	8
5.2.3	Per als tràmits classificats de categoria Baixa	8
5.2.4	Ús de segells de temps:	8
6	Criteris comuns per a l'establiment de mecanismes d'identificació i signatura electrònica, en la implantació de serveis electrònics.	9
6.1	Criteri general.....	9
6.2	Criteris d'aplicació de nivell alt de seguretat.	9
6.3	Criteri d'aplicació de nivell baix de seguretat	9
7	El Consorci AOC i la seguretat dels mecanismes de identificació i signatura	10

1 Introducció

El 23 de juliol de 2014 el Parlament Europeu i el Consell de la Unió Europea van aprovar el Reglament N° 910/2014 relatiu a la identificació electrònica i els serveis de confiança per les transaccions electròniques en el mercat interior, conegut com a ReldAS, que deroga l'antiga Directiva Europea 1999/93/CE de Signatura Electrònica i estableix les característiques i ús dels mecanismes d'identificació, signatura electrònica, i de tots aquells serveis de confiança que hi tenen relació. En concret, el Reglament 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, així com 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.

ReldAS descriu un esquema de tres nivells de seguretat per als mecanismes d'identificació, que queden definits al Reglament d'Execució de la Comissió Europea 2015/1502 de 8 de Setembre de 2015. També defineix quatre tipus de signatura i segell electrònic que cada Administració podrà acceptar i emprar d'acord als seus requisits normatius i de seguretat.

Per altra banda, 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 emprar per part de les Administracions, coherent i complementari al especificat a ReldAS. 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.

Pel que fa als mecanismes de signatura electrònica, La Llei 59/2003, de 19 de desembre, de Signatura Electrònica és la norma general que estableix les seves característiques i ús. Aquesta llei permet, en el seu article 4, que les administracions públiques facin ús de les tecnologies de signatura electrònica i, fins i tot, que estableixin condicions addicionals al seu ús per salvaguardar les garanties de cada procediment.

En l'àmbit de Catalunya, el Decret 56/2009, de 7 d'abril, per al impuls i el desenvolupament dels mitjans electrònics a l'Administració de la Generalitat de Catalunya, és la norma que desenvolupa les bases establertes per la Llei d'accés electrònic dels ciutadans als serveis públics. Més tard s'han aprovat la Llei 29/2010, de 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya, la Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya i el Decret 232/2013 de 15 d'octubre, per la qual es crea la Seu Electrònica, completen el cos normatiu dedicat a l'ús dels mitjans electrònics a Catalunya i són aplicables a totes les administracions catalanes.

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.

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.

El 20 de juliol del 2015 el Departament de Governació i Relacions Institucionals va aprovar el Protocol d'Identificació i Signatura Electrònica (ordre GRI/233/2015), que marca els criteris d'acceptació i ús dels diferents mecanismes en l'àmbit de l'Administració de la Generalitat de Catalunya. L'objecte d'aquesta guia és la de oferir un conjunt de criteris comuns similars a la resta d'administracions, en quan als aspectes tècnics i organitzatius necessaris per a la implantació dels sistemes de identificació i signatura electrònica per a cada tràmit o servei, als efectes de determinar el seu grau de seguretat.

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 Reglament Europeu 910/2014 relatiu a la identificació electrònica i els serveis de confiança, en endavant ReldAS, 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 els mecanismes disponibles en l'actualitat.

3.2 Signatura electrònica i segells electrònics

Aquests nivells de seguretat, d'acord amb ReldAS, no són aplicables als sistemes de signatura i segells electrònics. Aquests formen part del que el reglament anomena "serveis de confiança", i per tant són susceptibles de ser auditats i qualificats. La seva classificació es farà en base a les seves característiques i a aquesta qualificació, i es podran considerar els següents tipus:

- 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 ReldAS (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 categoria 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 descriuran 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 ciutadans

- Els certificats electrònics qualificats que hagin estat emesos per Prestadors de Serveis de Certificació (PSCs) inclosos a la Trusted Services List (TSL) publicada per l'òrgan competent de qualsevol país de la Unió Europea d'acord amb el que estableix ReldAS.
- S'hauran d'admetre, amb caràcter general, qualsevol dels mitjans d'identificació inclosos a la llista que 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, conforme al que estableix el mateix reglament.
- El certificat qualificat reconegut de signatura avançada idCAT per a ciutadà que emet el Consorci AOC.
- El mecanisme idCAT-SMS 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.

4.1.2 Per empreses

- Els certificats reconeguts emesos a una persona jurídica o a un ens sense personalitat i custodiats per una persona física, titular del certificat, la qual el pot emprar per actuar en nom de l'empresa o de l'ens indicat al certificat.
- Els certificats reconeguts emesos a una persona jurídica o a un ens sense personalitat, amb indicació expressa de la representació que ostenta la persona física titular del certificat.

- Els certificats de segell electrònic qualificat emesos a una persona jurídica o a un ens sense personalitat per Prestadors de Serveis de Certificació (PSCs) inclosos a la Trusted Services List (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.

4.1.3 Per als empleats públics

- El certificat reconegut o qualificat que el Consorci AOC emet al empleats del Sector Públic de Catalunya en dispositiu segur de creació de signatura: la T-CAT
- El certificat reconegut o qualificat que el Consorci AOC emet al empleats del Sector Públic de Catalunya en suport programari: la T-CAT P
- Els certificats reconeguts o qualificats emesos per prestadors inclosos a la "Llista de confiança de Prestadors de Serveis de Certificació (TSL)" publicada pel Ministerio de Industria, Energia y Turismo conforme al perfil "Empleado público" aprovat pel Consejo Superior de Administración Electrónica.
- D'altres sistemes no criptogràfics, com els usuaris i contrasenyes de la plataforma EACAT
- Qualsevol perfil de certificats reconeguts o qualificats emesos per prestadors inclosos a la "Llista de confiança de Prestadors de Serveis de Certificació (TSL)" publicada pel Ministerio de Industria, Energia y Turismo que acreditin la vinculació del seu titular a un ens públic.

4.1.4 Pels ens de l'administració davant dels ciutadans:

- Els certificats qualificats de seu electrònica i de servidor segur que el Consorci AOC emet als ens del Sector Públic de Catalunya.
- Els certificats electrònics qualificats emesos per altres Prestadors de Serveis de Certificació - diferents al Consorci AOC - inclosos a la Trusted Services List (TSL) del Ministerio de Industria Energía y Turismo 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.

4.2 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 que hagin estat emesos per Prestadors de Serveis de Certificació (PSCs) inclosos a la Trusted Services List (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 Llei de Signatura Electrònica 11/2007, d'accés electrònic dels ciutadans als Serveis Públics.
- El mecanisme idCAT-SMS com a mecanisme signatura electrònica dels ciutadans (persones físiques) no criptogràfic.

4.2.2 Per empreses

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

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'aquesta guia.

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 reconeguts o qualificats emesos per altres Prestadors de Serveis de Certificació inclosos a la Trusted Services List (TSL) del Ministerio de Industria Energía y Turismo 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, de Règim Jurídic del Sector Públic :
 - 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 reconeguts o qualificats de segell electrònic que el Consorci AOC emet als ens del Sector Públic de Catalunya.
- Els certificats reconeguts de persona jurídica que el Consorci AOC emet als ens del Sector Públic de Catalunya.
- Els certificats reconeguts de persona jurídica emesos als ens públics per altres Prestadors de Serveis de Certificació inclosos a la Trusted Services List (TSL) del Ministerio de Industria Energía y Turismo.

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;

- Els serveis publicats a la Seu electrònica del MINETUR, sota l'apartat "Otros servicios en relación con la firma electrónica - Servicios de validación temporal";
- 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.

4.2.6 Interoperabilitat de les signatures electròniques

Tal i com estableix l'article 45 de la Llei 40/2015 de Règim Jurídic del Sector Públic, quan una Administració empli 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 Admissió de mecanismes d'identificació i de signatura electròniques

5.1 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'Esquema Nacional de Seguretat en relació amb la Llei Orgànica de Protecció de Dades de Caràcter Personal.

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:

5.1.1 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 reconeguts o qualificats, que s'emeten 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'inclougi 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.

5.1.2 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 reconeguts o qualificats i els certificats reconeguts o 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'inclouï 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.
- El mecanisme idCAT-SMS.
- 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'Esquema Nacional de Seguretat i del Reglament d'Execució 2015/1502 de la Comissió Europea.

5.1.3 Per als tràmits classificats de categoria Baixa

Seràn admissibles els mecanismes d'identificació de nivell de seguretat baix, com aquells que fan un registre ordinari dels usuaris (que no inclouen la verificació fiable del document identificador oficial; ni la comprovació de les altres dades d'identificació personal i/o d'altres atributs que s'estableixin tots els requisits d'identificació establerts en els punts anteriors) o proveeixen els usuaris d'unes credencials de robustesa baixa.

5.2 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.

5.2.1 Per als tràmits classificats de categoria Alta

S'admeten signatures electròniques reconegudes o qualificades o segells electrònics reconeguts o 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 es definiran per a les signatures qualificades, 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 la interoperabilitat en l'accés transfronterer a serveis públics.
- Pel que fa als certificats emprats: s'han d'admetre les signatures electròniques generades amb aquells certificats reconeguts o 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 reconeguts o qualificats, entre els considerats a l'apartat 6.2, que s'emetin en un dispositiu qualificat de creació de segells electrònics. I atenen a les tipologies de certificats i que es llisten per a cadascun dels col·lectius que allà es distingeixen específic.

5.2.2 Per als tràmits classificats de categoria Substancial

Seràn admissibles les signatures electròniques avançades i els segells electrònics avançats que es fonamenten en un procediment de registre fiable de la identitat dels usuaris; també les signatures electròniques avançades basades en un certificat reconegut o qualificat de signatura electrònica i els segells electrònics avançats basats en certificats qualificats de segell electrònic, conforme al que estableix el ReIDAS als articles 27.1 i 37.1; 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 en l'ús transfronterer de serveis públics.
- 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 allà es distingeixen.
- Seràn admissibles les signatures ordinàries basades en el mecanisme idCAT SMS.
- També les signatures ordinàries basades en altre mecanismes que hagin estat classificat de nivell mig o substancial integrats com a tals al servei VÀlid operat pel Consorci AOC.

5.2.3 Per als tràmits classificats de categoria Baixa

S'admeten els mecanismes que generen signatures electròniques ordinàries prenent com a fonament un mecanisme d'identificació de nivell de seguretat baix, com els descrits a l'apartat 5.1.3.

5.2.4 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.

6 Criteris comuns per a l'establiment de mecanismes d'identificació i signatura electrònica, en la implantació de serveis electrònics.

6.1 Criteri general

S'estableix com criteri general que per a la identificació i signatura electrònica en els tràmits o serveis electrònics s'admetran els mecanismes d'identificació i signatura classificats amb nivell de seguretat mitjà o substancial, conforme als apartats 5.1.2 i 5.2.2.

6.2 Criteris d'aplicació de nivell alt de seguretat.

Es requerirà l'establiment d'un nivell de seguretat Alt en la implantació de sistemes d'identificació i signatura electrònica, per a l'establiment de tràmits o serveis electrònics que reuneixin algun d'aquests requisits:

- Identificació i signatura de tràmits que donin accés o transfereixin dades d'alt nivell de protecció segons l'article 7 de la LOPD o quan l'accés a dades pugui tenir una afectació a drets de tercers especialment protegits la LOPD.
- Identificació i signatura en el tràmit o procés de contractació, de conformitat amb la disposició addicional setzena f), de la Llei 59/2003, de 19 de desembre, de signatura electrònica".
- Identificació i signatura en el tràmit de concessió de subvenció o altres amb un contingut econòmic de més de 60.000€ o quan així estigui establert a les bases reguladores de les convocatòries.
- Aquells tràmits o procediments que la normativa específica estableixi amb un nivell alt d'identificació o signatura electrònica.

6.3 Criteri d'aplicació de nivell baix de seguretat

Es requerirà l'establiment d'un nivell de seguretat baix en els sistemes d'identificació i signatura electrònica, per a l'establiment de tràmits o serveis electrònics, que reuneixin algun d'aquests requisits:

- Identificació i/o signatura en tràmits de pagament o autoliquidacions de taxes i tributs.
- Petició de dret d'accés sol·licituds d'informació pública, sempre que el contingut de la petició no estigui sotmès a un nivell més elevat de seguretat.
- Tots els serveis i tràmits electrònics que suposin una actuació prevista en un procediment administratiu a excepció de les següents actuacions: formular sol·licituds, presentar declaracions responsables, interposar recursos, desistir d'accions o renunciar a dret i aquelles tràmits continguin una informació de un nivell més elevat de seguretat.
- Altres tràmits o procediments que la normativa específica estableix un sistema d'identificació i signatura de nivell més elevat de seguretat.

7 El Consorci AOC i la seguretat dels 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.