Núm. 7219

AJUNTAMENT D'OLOT

Anunci d'aprovació del Protocol d'identificació i signatura electrònica

Núm_referència X2018023214
Núm_expedient SG112018000008

La Junta de Govern Local en sessió de 26 de juliol de 2018, va aprovar el Protocol d'identificació i signatura electrònica, que es transcriu a continuació, que determina els aspectes tècnics i organitzatius necessaris per a la implantació dels sistemes de signatura electrònica per a cada tràmit o servei. Aquest acord entrarà en vigor l'endemà de la publicació en el Butlletí Oficial de la Província de Girona i es publicarà a la seu electrònica d'aquesta corporació.

L'Ajuntament d'Olot adaptarà els mecanismes d'identificació i de signatura electrònica dels seus serveis electrònics als criteris que s'hi estableixen en el termini d'un any des de la publicació d'aquest acord.

Els procediments relatius a serveis electrònics que s'hagin iniciat mantindran els mecanismes d'identificació i de signatura electrònica que s'hagin establert en les normes reguladores de cada tràmit, fins a la resolució final.

Contra la resolució transcrita, es podrà interposar potestativament recurs de reposició davant aquest mateix òrgan o ser impugnat directament davant la jurisdicció contenciosa administrativa.

El termini per la interposició del recurs serà d'un mes pel de reposició i de dos mesos pel contenciós administratiu, a partir, del dia següent al de la notificació d'aquesta resolució.

El termini per resoldre el recurs de reposició és d'un mes. En cas de desestimació per silenci administratiu del recurs de reposició, el termini per impugnar davant la jurisdicció contenciosa administrativa és de sis mesos.

Es podrà interposar també qualsevol altre recurs o procediment d'impugnació o reclamació previst en la legislació vigent.

Olot, 2 d'agost de 2018

Josep Berga i Vayreda
Alcalde accidental

Annex I. Protocol d'identificació i signatura electrònica

1. Introducció.

La Llei 59/2003, de 19 de desembre, de signatura electrònica es la norma general que regula les característiques i l'ús de la signatura electrònica. Aquesta Llei permet, d'acord amb l'article 4, que les administracions públiques facin ús dels mecanismes de signatura electrònica i que estableixin condicions addicionals al seu ús per salvaguardar les garanties de cada procediment. Aquesta llei ha estat en part modificada per la Llei 25/2015 de 28 de juliol, de mecanisme de segona oportunitat, reducció de la càrrega financera i altres mesures d'ordre social, en la seva disposició final quarta.

Per altra banda, la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, actualment derogada per la Llei 39/2015 d'1 d'octubre, del procediment administratiu comú de les administracions públiques, va establir els tipus de signatura a utilitzar per part de la ciutadania i de les administracions publiques quan es relacionen per mitjans electrònics.

La Llei d'accés electrònic dels ciutadans als serveis públics va ser objecte d'un desplegament reglamentari posterior.

En primer lloc, aquesta Llei va estar desenvolupada pel Reial decret 1671/2009, derogat parcialment per la Llei 39/2015, pel qual es desplegava parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, el qual va introduir determinades obligacions relacionades amb l'ús de la signatura electrònica per a les administracions d'àmbit estatal. Aquest Reial decret s'aplica a les administracions catalanes de forma supletòria, es a dir, en aquells casos en que no hi hagi una norma pròpia d'àmbit autonòmic que cobreixi un determinat supòsit de fet.

Actualment és en l'articulat de la Llei 39/2015, del procediment administratiu comú de les administracions públiques, concretament en l'article 9 i següents, on s'estableixen els sistemes d'identificació dels interessats en el procediment, els sistemes de signatura admesos per les administracions públiques, així com l'ús de mitjans i signatura en el procediment administratiu.

En segon lloc, s'han aprovat l'Esquema Nacional de Seguretat i l'Esquema Nacional d'Interoperabilitat (Reial decret 3/2010 i Reial decret 4/2010, respectivament), pels quals es desplega la Llei d'accés electrònic dels ciutadans als serveis públics en aspectes puntuals relacionats amb la gestió dels sistemes d'informació de les administracions publiques. Aquests documents estableixen unes bases comunes per a totes les administracions públiques per tal d'assegurar la interoperabilitat entre els sistemes d'informació tot garantint la normalització, la seguretat i la conservació de la informació.

El contingut de les disposicions de l'Esquema Nacional de Seguretat i de l'Esquema Nacional d'Interoperabilitat és incorporat en els diferents apartats d'aquest Protocol i, particularment, s'integren en l'avaluació dels riscos per a la determinació dels sistemes de signatura que es vulguin utilitzar.

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 regim jurídic i de procediment de les administracions publiques de Catalunya, l'Ordenança reguladora de l'Administració electrònica de l'Ajuntament d'Olot (aprovada per Acord de Ple de l'Ajuntament d'Olot, en la sessió ordinària celebrada el dia 26 de juliol de 2012), són els textos que completen el cos normatiu regulador de l'ús dels mitjans electrònics.

2. Objecte del Protocol.

L'objecte d'aquest Protocol es establir els criteris comuns a l'Ajuntament d'Olot pel que fa als aspectes tècnics i organitzatius necessaris per a la implantació dels sistemes d'identificació i signatura electrònica per a cada tràmit o servei, en funció del seu grau de seguretat.

3. Àmbit d'aplicació.

Aquest Protocol s'aplica als tràmits o procediments que es produeixen en les relacions entre l'Ajuntament d'Olot i els ciutadans i ciutadanes, i en les relacions entre els diferents òrgans administratius, en els àmbits següents:
a) En l'àmbit de les relacions interadministratives.
b) En l'àmbit de les relacions interorgàniques.

4. Òrgans competents.

La unitat de Serveis Generals (Administració electrònica), com a òrgan competent en el foment de l'administració electrònica de l'Ajuntament, es l'òrgan responsable de:
a) Elaboració, execució i realitzar el seguiment del present Protocol.
b) Impuls de serveis o tràmits electrònics.

5. Identitat electrònica i signatura electrònica.

Als efectes de determinar la identitat i signatura electrònica adequada al grau de seguretat de cada tràmit o servei electrònic, aquest Protocol estableix:

1. Els mecanismes d'identificació i signatura electrònica aplicables per a cada tràmit i servei d'acord amb el Reglament europeu 910/2014 relatiu a la identificació electrònica i els serveis de confiança (en endavant ReIdAS) i les normatives autonòmiques i estatals en matèria d'identificació i signatura electrònica.

2. Els mecanismes de signatura electrònica i segell electrònic, d'acord amb el que determinen les seccions 4 i 5 del ReIdAS, que s'estableixen en el punt 6 d'aquest Protocol són:
- Signatures i segells electrònics.
- Signatures i segells electrònics avançats.
- Signatures i segells electrònics avançats basats en certificats qualificats.
- Signatures i segells electrònics qualificats.

3. L'Admissió dels mecanismes d'identificació i signatura electrònica segons la classificació dels nivells de seguretat que determina l'article 8 del ReIDAS i altres normes estatals en matèria de seguretat, que s'estableixen en el punt 7.
Aquests mecanismes es classifiquen en tres nivells de seguretat:
- Nivell de seguretat baix, amb l'objectiu de reduir el risc d'us indegut o alteració de la identitat presentada.
- Nivell de seguretat substancial, amb l'objectiu de reduir substancialment el risc d'us indegut o alteració de la identitat.
- Nivell de seguretat alt, amb l'objectiu d'evitar l'ús indegut o l'alteració de la identitat.

4. Criteris generals per a la determinació del grau de seguretat que requereix un tràmit o servei electrònic, que s'estableixen en el punt 8 d'aquest Protocol.

5. L'òrgan competent en el desenvolupament d'un servei electrònic determinarà els mecanismes d'identificació o de signatura electrònica que siguin pertinents per a cada tràmit, atesa la diversa funcionalitat d'ambdós mecanismes electrònics.

6. De conformitat amb l'article 26.b) del ReIDAS i l'article 3 de la Llei de 59/2003 de signatura electrònica, la signatura electrònica ha de permetre la identificació de la persona que signa el document. L'òrgan competent en la creació del servei, d'acord amb la normativa de procediment administratiu aplicable, determinarà si es requereixen exclusivament mecanismes de signatura per a la producció dels dos efectes.

6. Mecanismes d'identificació i signatura electrònica.

Els mecanismes d'identificació i signatura electrònica per acreditar la identitat d'usuaris i signataris per mitjans electrònics es determinarà en funció del subjecte i el grau de seguretat del tràmit corresponent.

Els mecanismes admesos són:

6.1 Mecanismes d'identificació.

6.1.1 Per a persones físiques.
- Els certificats electrònics qualificats que hagin estat emesos per prestadors de serveis de certificació (PSCs) 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 publicarà la Comissió Europea per accedir als serveis prestats en línia per un organisme del sector públic en un estat membre, a l'efecte de l'autenticació transfronterera, conforme al que estableix el ReIdAS.
- El certificat qualificat de signatura avançada idCAT per als ciutadans que emet el Consorci AOC.
- Els certificats del DNI electrònic, d'acord amb el que estableix la Llei 39/2015, del procediment administratiu comú de les administracions públiques.
- El mecanisme idCAT-SMS, que es un mecanisme d'identificació i signatura electrònica dels ciutadans (persones físiques) no criptogràfic, basat en l'enviament de codis d'un sol us a dispositius mòbils, gestionat pel Consorci AOC.

6.1.2 Per a persones jurídiques.
- Els certificats reconeguts o qualificats emesos a favor d'una persona jurídica o un ens sense personalitat jurídica 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 en el certificat.
- Els certificats qualificats emesos a favor d'una persona jurídica o un ens sense personalitat jurídica, 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 a un ens sense personalitat per prestadors de serveis de certificació (PSCs), 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. Aquesta representació es podrà verificar mitjançant la consulta a un registre en línia de representacions, especialment, mitjançant el servei REPRESENTA del Consorci AOC.

6.1.3 Per als empleats públics.
- El certificat reconegut o qualificat que el Consorci AOC emet als 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 als empleats del sector públic de Catalunya en suport programari: la T-CAT P.
- Els certificats reconeguts o qualificats emesos per prestadors inclosos en la TSL, publicada pel Ministeri d'Indústria, Energia i Turisme conforme al perfil "Empleat públic" aprovat pel Consell Superior d'Administració Electrònica.
- Altres sistemes no criptogràfics, com ara els usuaris i contrasenyes de les plataformes EACAT i GICAR.
- Excepcionalment, el DNI electrònic, d'acord amb la Llei 39/2015, del procediment administratiu comú de les administracions públiques.
- Es podran facilitar certificats qualificats de signatura electrònica amb pseudònim en aquells casos en que siguin aplicables límits a la identificació de les persones signants dels documents, derivats de la legislació vigent. El pseudònim s'instrumentarà mitjançant l'ús del número d'identificació professional o equivalent.
- L'Ajuntament d'Olot podrà establir mecanismes de signatura electrònica manuscrita amb captura de dades biomètriques, per al seu ús, en relacions presencials, per a les persones al seu servei. Aquests mecanismes han de garantir, en tot cas, la confidencialitat de les dades de representació de la signatura, així com la no reutilització de les mateixes per part de l'Ajuntament d'Olot o de terceres persones, i la integritat i inalterabilitat de les dades signades.

6.1.4 Altres mecanismes d'identificació.
La incorporació de nous mecanismes d'identificació electrònica, quan aquests mecanismes estiguin disponibles en el mercat per als usuaris del seu àmbit subjectiu, s'ha de fer d'acord amb el procediment establert en el punt 8.5 d'aquest Protocol.

6.2 Mecanismes de signatura i segell electrònic.

S'admetrà l'ús dels mecanismes de signatura i segell electrònic de les persones, dels empleats públics que, de conformitat amb el que estableix l'article 27 del ReIDAS:
- siguin conformes a algun dels formats de referència que definirà la Comissió Europea per a les signatures avançades;

Així mateix, s'admetran altres mecanismes que es classifiquin d'acord amb aquest Protocol.

6.2.1 Per a persones físiques.
- Els certificats electrònics 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.
- El certificat reconegut o qualificat de signatura avançada idCAT que emet el Consorci AOC.
- Els certificats del DNI electrònic, d'acord amb el que estableix la Llei 39/2015, del procediment administratiu comú de les administracions públiques.
- El mecanisme idCAT-SMS com a mecanisme de signatura electrònica dels ciutadans (persones físiques) no criptogràfic.
- L'Ajuntament d'Olot podrà establir mecanismes de signatura manuscrites amb captura de dades biomètriques per al seu ús en relacions presencials amb les persones físiques. Aquests mecanismes hauran de garantir, en qualsevol cas, la confidencialitat de les dades de representació de la signatura, així com la no reutilització dels mateixos per part de l'entitat local o de terceres persones, i la integritat i inalterabilitat de les dades signades.

6.2.2 Per a persones jurídiques.
Les persones jurídiques i els ens sense personalitat jurídica podran generar signatures electròniques amb els mecanismes d'identificació detallats en el punt 6.1.2 d'aquest Protocol.

6.2.3 Per als empleats públics.
Els empleats públics podran generar signatures electròniques amb els mecanismes d'identificació detallats en el punt 6.1.3 d'aquest Protocol.
Es recomana que, quan els empleats públics utilitzin signatures electròniques amb sistemes no criptogràfics, aquestes sistemes es formalitzin mitjançant l'ús d'un segell electrònic i, si escau, amb codi segur de verificació.

6.2.4 Segells de temps.
Les signatures electròniques avançades incorporen segells de temps generats per algun dels serveis següents:
- El servei segell de temps del Consorci AOC.
- Els serveis publicats a la seu electrònica del Ministeri d'Industria, Energia i Turisme en l'apartat "Altres serveis en relació amb la signatura electrònica - Serveis de validació temporal".
- Qualsevol altre servei de segell de temps qualificat conforme al 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.

6.2.5 Altres mecanismes de signatura.
Per tal d'afavorir la interoperabilitat i possibilitar la verificació automàtica de la signatura electrònica dels documents electrònics autenticats amb sistemes que no es basen en certificats qualificats, l'Ajuntament d'Olot podrà superposar el seu propi segell electrònic avançat en certificat electrònic qualificat als documents per a, posteriorment, remetre'ls o posar-los a disposició d'altres òrgans, organismes públics, entitats de dret públic o administracions.
La incorporació de nous mecanismes de signatura electrònica, com ara els mecanismes de signatura biomètrica, quan aquests estiguin disponibles en el mercat per als usuaris del seu àmbit subjectiu, s'ha de fer conforme al procediment establert en el punt 8.5 d'aquest Protocol.

7. Admissió de mecanismes d'identificació i signatura electrònica.

7.1 Admissió de mecanismes d'identificació electrònica.

Amb caràcter general, els ciutadans i ciutadanes es poden identificar electrònicament davant de l'Ajuntament d'Olot emprant qualsevol sistema d'identificació que compti amb un registre previ com a usuari que permeti garantir la seva identitat.

L'Admissió dels mecanismes d'identificació i signatura electrònica es du a terme conforme als nivells de seguretat requerits en l'Esquema Nacional de Seguretat.

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

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

7.1.1 Per als tràmits classificats amb categoria alta.
S'admeten els sistemes d'identificació electrònica de nivell de seguretat alt, que són els 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:
- Els certificats reconeguts o qualificats que s'emetin en un dispositiu qualificat de creació de signatura electrònica, d'entre els establerts en el punt 6 d'aquest Protocol, atenent a les tipologies de certificats i del col·lectiu específic.
- Qualsevol dels mitjans d'identificació que hagi estat classificat amb nivell de seguretat alt i s'inclogui en la llista que, conforme al que estableix el ReIDAS en el capítol 2, publicarà la Comissió Europea per accedir als serveis prestats en línia per un organisme del sector públic en un estat membre, a l'efecte de l'autenticació transfronterera.

7.1.2 Per als tràmits classificats amb categoria mitjana o substancial.
S'admeten els sistemes d'identificació electrònica de nivell de seguretat mitjana o substancial, que són els que fan un registre fiable dels usuaris, el qual es podrà dur a terme de manera presencial o remota (en línia), i proveeixen els usuaris d'unes credencials de robustesa substancial. Concretament,
a. Obligatòriament, els certificats reconeguts o qualificats i els certificats reconeguts o qualificats de segell electrònic establerts en el punt 6 d'aquest Protocol, atenent a les tipologies de certificats i del col·lectiu específic.
b. Obligatòriament, qualsevol dels mitjans d'identificació que hagi estat classificat amb nivell de seguretat substancial i s'inclogui a la llista que, conforme al que estableix el ReIDAS en el capítol 2, publicarà la Comissió Europea per accedir als serveis prestats en línia per un organisme del sector públic en un estat membre, a l'efecte de l'autenticació transfronterera.
c. El mecanisme idCAT-SMS.
d. Qualsevol altre mecanisme que hagi estat classificat amb nivell mitjà, d'acord amb el que estableix aquest Protocol.

7.1.3 Per als tràmits classificats amb categoria baixa.
Són admissibles els mecanismes d'identificació de nivell de seguretat baix, que són els 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) o proveeixen els usuaris d'unes credencials de robustesa baixa.

7.2 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 que vulguin 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 a l'Ajuntament d'Olot, 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 amb una categoria determinada són també admissibles per a les actuacions classificades de categoria inferior.

En particular, quan en el context d'un servei electrònic de l'Ajuntament d'Olot es requereixi una signatura electrònica per garantir la protecció de la integritat i de l'autenticitat de les dades o dels documents implicats, s'admetran les signatures següents:

7.2.1 Per als tràmits classificats amb categoria alta.
S'admeten signatures electròniques reconegudes o qualificades o segells electrònics reconeguts o qualificats, segons correspongui, amb caràcter obligatori:
- Quant 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 l'article 27 del ReIDAS, a l'efecte de garantir la interoperabilitat en l'accés transfronterer als serveis públics.
- Pel que fa als certificats emprats, s'han d'admetre les signatures electròniques generades amb els certificats reconeguts o qualificats de signatura electrònica, d'entre els previstos en l'apartat 6.2 d'aquest Protocol, que s'emetin en un dispositiu qualificat de creació de signatura electrònica. També els segells electrònics generats amb els certificats de segell electrònic reconeguts o qualificats, d'entre els previstos en l'apartat 6.2 d'aquest Protocol, que s'emetin en un dispositiu qualificat de creació de segells electrònics, atenent a les tipologies de certificats i del col·lectiu específic.

7.2.2 Per als tràmits classificats de categoria mitjana o substancial.
Seran admissibles les signatures electròniques avançades i els segells electrònics avançats que es fonamentin 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, d'acord amb el que estableix el ReIDAS en els 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 ara els considerats en l'apartat 6.1.2 d'aquest Protocol o altres que es puguin incorporar conforme a l'apartat 8.5.

Concretament,

- Quant als formats, els serveis electrònics oferts pels organismes dels estats membres de la Unió Europea han 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 que es definiran per a les signatures electròniques avançades, o que s'hagin generat amb els mètodes de referència quan siguin d'un format alternatiu, d'acord amb el que estableix l'article 27 del ReIDAS, a l'efecte de garantir el correcte tractament dels documents signats electrònicament en l'ús transfronterer dels serveis públics.
- Pel que fa als certificats emprats, s'han d'admetre les signatures electròniques generades amb els certificats de signatura electrònica considerats en l'apartat 6.2 d'aquest Protocol. També els segells electrònics generats amb els certificats de segell electrònic considerats en el mateix apartat 6.2 d'aquest Protocol, atenent a les tipologies de certificats que es detallen per a cadascun dels col·lectius que s'hi especifiquen.
- Seran admissibles les basades en el mecanisme idCAT SMS.
- Qualsevol altre mecanisme d'identificació i signatura electrònica 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 pel Reglament d'Execució 2015/1502 de la Comissió Europea.
- Qualsevol altre mecanisme que hagi estat classificat amb nivell mitjà, d'acord amb el que estableix aquest Protocol.

7.2.3 Per als tràmits classificats amb categoria baixa.
S'admeten els mecanismes que generen signatures electròniques ordinàries a partir d'un mecanisme d'identificació de nivell de seguretat baix, com ara els descrits en l'apartat 7.1.3 d'aquest Protocol o altres que es puguin incorporar d'acord amb l'apartat 8.5.

7.2.4 Us de segells de temps.
S'admeten les signatures electròniques avançades que incorporen segells de temps generats per algun dels serveis descrits en l'apartat 6.2.5 d'aquest Protocol.

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

8.1 Criteri general.

S'estableix com criteri general que, per a la identificació i la signatura electrònica en els tràmits o serveis electrònics, s'admetran els mecanismes d'identificació i signatura classificats amb nivell de seguretat mitja o substancial, conforme als apartats 7.1.2 i 7.2.2 d'aquest Protocol.

8.2 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 normativa vigent de protecció de dades de caràcter personal o quan l'accés a les dades pugui afectar els drets de terceres persones especialment protegides per aquesta normativa.
- Identificació i signatura en el tràmit de contractació especificat per cada fase per l'òrgan de contractació atenent als riscos associats a l'intercanvi d'informació.
- Identificació i signatura en el tràmit o procés de concessió de subvencions o altres tràmits amb un contingut econòmic de més de 60.000 EUR o quan així estigui establert en les bases reguladores de les convocatòries.
- Els tràmits o procediments que la normativa específica estableixi amb un nivell alt d'identificació o signatura electrònica.

8.3.- 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 tràmits o serveis electrònics que reuneixin algun d'aquests requisits:

- Identificació i/o signatura en tràmit de pagament o autoliquidacions de taxes o tributs.
- Tots el tràmits electrònics o serveis electrònics d'un procediment d'un procediment administratiu, a excepció de les actuacions següents:
  Formular sol·licituds, presentar declaracions responsables, interposar recursos, desistir d'accions o renunciar a drets, així com aquells tràmits que continguin una informació d'un nivell més elevat de seguretat.
- Altres tràmits o procediments en què la normativa específica estableix un sistema d'identificació i signatura de nivell baix de seguretat.

8.4 Criteris de selecció del nivell de seguretat.

Els òrgans que impulsin o modifiquin serveis seleccionaran el nivell de seguretat que cada tipus d'actuació requereix en base al que fixa aquest protocol, atenent a criteris de seguretat i garantia jurídica.

8.5 Establiment de nivell de seguretat d'altres mecanismes

L'acceptació de nous mecanismes de identificació i signatura electrònica d'acord al que descriu aquest Protocol, així com l'establiment del seu nivell de seguretat, es basarà en la informació de classificació que publica el Consorci AOC al seu lloc web.