

RESOLUCIÓ

Núm. expedient	2017-D225-0007		
Objecte	Aprovació de la política de signatura electrònica del Consorci de les Drassanes Reials i Museu Marítim de Barcelona		
Destinatari			
CIF/DNI		Import total	
Acte de referència VNIS		Altres serveis	

1. Necessitats d'una política de signatura electrònica

Vist que el Consorci de les Drassanes Reials i Museu Marítim de Barcelona, té la voluntat de dissenyar una política de signatura electrònica en relació al procediments i serveis electrònics que presta.

Vist que el Consorci de les Drassanes Reials i Museu Marítim de Barcelona és una entitat administrativa de caràcter local i que com a Administració Pública, presta una sèrie de serveis públics, i alhora és relaciona amb altres Administracions públiques i ciutadans, mitjançant procediments electrònics, i en aquest marc d'interoperabilitat es requereix l'adopció d'una política de signatura d'acord amb els requisits de seguretat i proporcionalitat que estableix la normativa vigent.

2. Normativa

- Reglament N. 910/2014, de 23 de juliol de 2014, aprovat pel Parlament Europeu i el Consell de la Unió Europea, relatiu a la identificació electrònica i els serveis de confiança per les transaccions electròniques en el mercat interior, conegut com a eIDAS, que deroga l'antiga Directiva Europea 1999/93/CE de Signatura Electrònica i estableix les característiques i l'ús dels mecanismes d'identificació, signatura electrònica, i de tots aquells serveis de confiança que hi tenen relació. En concret, a l'article 1 del Reglament esmentat, s'estableix 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 i les condicions en què s'han d'admetre els sistemes d'identificació electrònica de persones físiques i jurídiques que donen servei en

d'altres Estats membres. Tanmateix, 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, així com es defineixen quatre tipus de signatura i segell electrònic que cada Administració podrà acceptar i emprar d'acord als seus requisits normatius i de seguretat.

- Reglament d'Execució de la Comissió Europea 2015/1502 de 8 de Setembre de 2015, defineix i desenvolupa tres nivells de seguretat per als mecanismes d'identificació, d'acord amb els paràmetres de ReldAS.
- 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 emprar per part de les Administracions, coherent i complementari a l'especificat al ReldAS.
- La Llei 59/2003, de 19 de desembre, de Signatura Electrònica és la norma general que estableix els mecanismes de signatura electrònica, 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 es disposa del Decret 56/2009, de 7 d'abril, per a l'impuls i el desenvolupament dels mitjans electrònics a l'Administració de la Generalitat de Catalunya, que és la norma que desenvolupa les bases establertes a la Llei d'accés electrònic dels ciutadans als serveis públics, 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, i que completen el cos normatiu dedicat a l'ús dels mitjans electrònics a Catalunya i que són d'aplicació a totes les administracions catalanes.

Atès que aquesta política de signatura electrònica resulta aplicable als sistemes d'informació en què es gestionin els procediments administratius per mitjans electrònics, a les relacions amb els ciutadans a través de la seu electrònica del Consorci, i a l'intercanvi de documents i expedients d'acord amb el que estableix el Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Interoperabilitat en l'àmbit de l'Administració Electrònica.

3. Continguts de la Política de signatura electrònica de l'MMB

Vist que des de l'Arxiu General del Consorci s'ha redactat la política de signatura electrònica del Consorci de les Drassanes Reials i Museu Marítim de Barcelona, amb el següent contingut:

1 INTRODUCCIÓ

- 1.1 Objecte
- 1.2 Marc normatiu
- 1.3 Ambit d'aplicació
- 1.4 Dades d'identificació de la política de signatura electrònica
- 1.5 Actors involucrats

2 MECANISMES D'IDENTIFICACIÓ I SIGNATURA ELECTRÒNICA

- 2.1 Tipologia de mecanismes d'identificació i signatura electrònica disponibles
- 2.2 Mecanismes d'identificació i signatura electrònica en relació amb la tipologia de l'acte
 - 2.2.1 Identificació i signatura de la ciutadania en las seves relacions amb l'MMB
 - 2.2.2 Identificació i signatura per a les actuacions administratives dels òrgans de l'MMB

3 RELACIÓ ENTRE LA SIGNATURA I EL DOCUMENT SIGNAT

4 FORMAT I PERFIL DE LA SIGNATURA

5 PROCESSOS EN RELACIÓ A LA SIGNATURA ELECTRÒNICA

Vist l'article el 18.2 en relació al 18.3 dels Estatuts pels quals es regeix aquest Consorci, el Director general adopta la següent

RESOLUCIÓ

PRIMER- APROVAR la Política de signatura electrònica del Consorci de les Drassanes Reials i Museu Marítim de Barcelona, elaborat per l'Arxiu, i que s'adjunta.

SEGON- DONAR COMPTE en la propera sessió del Consell General.

Barcelona, 16 de juny de 2017

Vist

L'Interventor delegat

Carles Bayén Fernández

Barcelona, 16 de juny de 2017
El Director general

Roger Marcet i Barbé

Política de signatura electrònica

Control de canvis
v.01

1	INTRODUCCIÓ.....	3
1.1	Objecte	3
1.2	Marc normatiu	3
1.3	Ambit d'aplicació	4
1.4	Dades d'identificació de la política de signatura electrònica	4
1.5	Actors involucrats.....	4
2	MECANISMES D'IDENTIFICACIÓ I SIGNATURA ELECTRÒNICA.....	5
2.1	Tipologia de mecanismes d'identificació i signatura electrònica disponibles.....	5
2.2	Mecanismes d'identificació i signatura electrònica en relació amb la tipologia de l'acte 7	
2.2.1	Identificació i signatura de la ciutadania en las seves relacions amb l'MMB.....	7
2.2.2	Identificació i signatura per a les actuacions administratives dels òrgans de l'MMB	8
3	RELACIÓ ENTRE LA SIGNATURA I EL DOCUMENT SIGNAT.....	9
4	FORMAT I PERFIL DE LA SIGNATURA.....	11
5	PROCESSOS EN RELACIÓ A LA SIGNATURA ELECTRÒNICA.....	11

1 INTRODUCCIÓ

1.1 OBJECTE

La present Política conté les Normes de signatura electrònica en relació amb els documents de procediments administratius electrònics del Consorci de les Drassanes Reials i Museu Marítim de Barcelona (MMB).

La naturalesa del Museu, el servei que presta i la necessitat d'interoperar amb altres administracions, exigeixen adoptar una política de signatura d'acord amb els requisits de seguretat i proporcionalitat que estableix la normativa vigent.

1.2 MARC NORMATIU

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 i les condicions en què 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 a emprar per part de les Administracions, coherent i complementari a l'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.

1.3 ÀMBIT D'APLICACIÓ

Aquesta política resulta aplicable als sistemes d'informació en què es gestionin procediments administratius per mitjans electrònics, a les relacions amb els ciutadans a través de la seu electrònica del Museu, i l'intercanvi de documents i expedients d'acord amb el que estableix el Reial decret 4/2010, Esquema nacional d'interoperabilitat.

1.4 DADES D'IDENTIFICACIÓ DE LA POLÍTICA DE SIGNATURA ELECTRÒNICA

La política de signatura electrònica v.1.0 s'ha emès pel Director General del Museu Marítim de Barcelona, actuant en virtut de les seves competències establertes en l'Article 18.3 dels estatuts de l'MMB publicats al BOPB del 15 de gener del 2016.

Les dades d'identificació d'aquesta política de signatura electrònica són:

Nom del document	Política de signatura electrònica del Consorci de les Drassanes Reials i Museu Marítim de Barcelona (MMB)
Versió	03
Data d'expedició	
Àmbit d'aplicació	Relacions entre ciutadans i MMB en els tràmits que es realitzen a través de la seu electrònica

El manteniment actualitzat de la política de signatura electrònica correspondrà a la Direcció General de l'MMB.

1.5 ACTORS INVOLUCRATS

Els actors involucrats en el procés de creació i validació de signatura electrònica són:

- Signant: persona que disposa d'un dispositiu de creació de signatura i que actua en nom propi o en nom d'una persona física o jurídica a la que representa.
- Verificador: entitat, persona física o jurídica, que valida o verifica una signatura electrònica mitjançant el contrast amb les condicions exigides per una Política de signatura concreta. Pot ser una entitat de validació de confiança o una tercera part que estigui interessada en conèixer la validesa d'una signatura electrònica.
- Prestador de serveis de signatura electrònica: la persona física o jurídica que expedeix certificats electrònics o presta altres serveis en relació amb la signatura electrònica.
- Emissor de la Política de Signatura Electrònica: entitat que s'encarrega de generar o gestionar el document de Política de Signatura Electrònica, mitjançant el qual quedaran vinculats el signant i el verificador en els processos de generació i validació de la signatura electrònica.

2 MECANISMES D'IDENTIFICACIÓ I SIGNATURA ELECTRÒNICA

2.1 TIPOLOGIA DE MECANISMES D'IDENTIFICACIÓ I SIGNATURA ELECTRÒNICA DISPONIBLES

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 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 ús a dispositius mòbils, operat pel 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.

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 ReldAS.
- 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.

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 d'acord 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.

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 ReldAS, emesos a nom d'un ens.
- Els certificats qualificats de segell electrònic que el Consorci AOC emet als ens del Sector Públic de Catalunya.
- 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 :
 - o 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 s'escau, 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.

o 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.

2.2 MECANISMES D'IDENTIFICACIÓ I SIGNATURA ELECTRÒNICA EN RELACIÓ AMB LA TIPOLOGIA DE L'ACTE

Els mecanismes d'identificació i signatura electrònica varien en funció de la transcendència de l'acte que es du a terme. L'objectiu d'aquesta Política de Signatura Electrònica és indicar els usos i condicions que es contemplen per a l'àmbit i abast concret del Museu Marítim de Barcelona, d'acord amb la normativa vigent.

2.2.1 Identificació i signatura de la ciutadania en les seves relacions amb l'MMB

L'ordre GRI/233/2015, de 20 de juliol, per la qual s'aprova el Protocol d'identificació i signatura electrònica, en el seu apartat 8.3, estableix que es requerirà l'establiment d'un nivell de seguretat baix en els sistemes d'identificació i signatura electrònica per a tots els tràmits electrònics o serveis electrònics d'un procediment administratiu, a excepció de les actuacions següents:

- Formular sol·licituds
- Presentar declaracions responsables,
- Interposar recursos,
- Desistir d'accions
- Renunciar a drets

La Llei 39/2015 d'1 d'octubre, del procediment administratiu comú de les administracions públiques, en els seus articles 9 i 10, diferencia els processos d'identificació i de signatura, per als quals es podran utilitzar sistemes diferents. Igualment, l'article 11 de la mateixa norma, estableix que amb caràcter general, per a la realització de qualsevol actuació prevista en el procediment administratiu, serà suficient que els interessats acreditin prèviament la seva identitat - dels definits en l'article 9.2-, i fa obligatori l'ús de signatura electrònica per les actuacions ja mencionades.

La identificació i acreditació de la voluntat de la ciutadania en les seves relacions amb el Museu Marítim de Barcelona es pot produir a través dels següents instruments o mecanismes:

- Autenticació amb certificat qualificat o reconegut.
- idCAT. És un mecanisme ofert pel Consorci AOC basat en l'enviament de contrasenyes d'un sol ús al telèfon mòbil de l'usuari, prèviament registrat.
- Cl@ve. És el sistema d'identificació d'usuaris emprat i ofert per l'Administració General de l'Estat.
- Les persones físiques podran, en tot cas i amb caràcter universal, utilitzar els sistemes de signatura electrònica incorporats al document nacional d'Identitat en la seva relació per mitjans electrònics amb l'MMB. El règim d'ús i efectes de l'esmentat document es regirà per la seva normativa reguladora.

2.2.2 Identificació i signatura per a les actuacions administratives dels òrgans de l'MMB

En relació amb la identificació, autenticació i signatura electrònica dels òrgans administratius de l'MMB, d'acord amb l'article 43.2 de la Llei 40/2015, d'1 d'octubre, de règim jurídic del Sector Públic, en relació amb l'article 3 de la Llei de Signatura Electrònica 59/2003, de 19 de desembre, cada administració pública determinarà els sistemes de signatura electrònica que ha d'utilitzar el seu personal, els quals podran identificar de manera conjunta el titular del lloc de treball o càrrec i l'Administració o òrgan en què presta els seus serveis.

- Per a les actuacions administratives manuals (que necessiten intervenció personal i directa del titular de l'òrgan administratiu) de nivell alt, l'MMB ha de facilitar al personal que hagi de signar i als alts càrrecs, un certificat electrònic que identificarà de forma conjunta el titular del lloc o càrrec i l'òrgan en què presta serveis. Per a les actuacions administratives manuals de nivell alt, el personal de l'MMB que hagi de signar, utilitzar 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, així com altres sistemes no criptogràfics, com ara els usuaris i contrasenyes de la plataforma EACAT
- Per a les actuacions administratives automatitzades de nivell alt, que no necessiten intervenció personal i directa del titular de l'òrgan administratiu, s'utilitzaran certificats electrònics que han d'incloure informació sobre la identificació de l'òrgan responsable del tràmit. 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
- Les signatures electròniques avançades incorporen segells de temps generats pel servei segell de temps del Consorci AOC

Es consideren actuacions administratives de nivell alt:

- 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 per la LOPD.

- 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”.
- 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 altres tràmits o procediments que la normativa específica de l'MMB estableixi amb un nivell alt d'identificació o signatura electrònica.

Els actes d'intercanvi de dades amb les administracions públiques, o l'accés a les dades d'aquestes, exigirà el nivell mínim establert per cada Administració que cedeix dades o dóna accés a dades.

La signatura electrònica dels actes de contractació pública i de facturació electrònics serà la que determini la normativa que li sigui aplicable.

La resta d'actes es poden documentar amb qualsevol sistema de signatura electrònica i en aquells que es determini mitjançant els sistemes d'autenticació basats en usuari i contrasenya. En l'MMB es consideren tràmits de nivell baix els 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 en 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:
 - o formular sol·licituds,
 - o presentar declaracions responsables,
 - o interposar recursos,
 - o desistir d'accions o renunciar a drets.

3 RELACIÓ ENTRE LA SIGNATURA I EL DOCUMENT SIGNAT

Un document electrònic no s'ha d'entendre com una cosa aïllada, sinó com un element dins d'un procediment administratiu, relacionat a un sistema d'informació, que ha de vetllar pel cicle de vida complet dels documents, respectant a més el que s'estableix en la política de gestió de documents de l'MMB. Si bé sobre un document aïllat és possible realitzar una signatura en un format adequat per permetre la seva conservació, s'ha de

considerar que l'existència de documents deslligats d'un sistema d'informació o del repositori documental de l'MMB pot ocasionar la pèrdua d'informació que garanteixi la seva autenticitat, integritat, confidencialitat, disponibilitat i traçabilitat, impedit per tant la protecció, recuperació i conservació física i lògica del document i el seu context

El format de la signatura ha de ser, sempre que sigui possible, independent del format del document o registre signat, amb l'objectiu de reduir al màxim la dependència entre tots dos objectes de negoci. Els certificats i les informacions d'estat es podran emmagatzemar dins el document resultant de la signatura electrònica (seguint les modalitats A TS-X o -A) o en un repositori específic (segellant de forma independent)

La relació entre el document signat i la signatura s'ha d'establir mitjançant l'ús de metadades del document.

Quan calgui lliurar a tercers aquests documents, s'ha de crear una còpia autèntica electrònica, en un format adient al destinatari, que serà signada o segellada electrònicament, embolcallant la signatura o segell en el format documental. (exemple: un fitxer PDF signat o segellat)

Es recomana que, addicionalment, els documents incorporin un codi de verificació electrònica, que permeti la seva consulta en línia i la impressió en concepte de còpia autèntica.

En relació amb els actes d'intercanvi de dades o accés a dades entre Administracions, la relació entre la signatura electrònica i el document signat serà típicament establerta per cada Administració que cedeix dades o dona accés a dades, sense perjudici d'establir aquestes condicions per conveni.

En relació amb els actes dels ciutadans, amb caràcter general es faran servir formularis amb signatura electrònica, tret que, d'acord amb la naturalesa de l'acte expressament se'n determini qualsevol altre mecanisme de relació.

Respecte als documents ofimàtics, signats o no, que puguin presentar els ciutadans acompanyant a la sol·licitud administrativa, no se'ls hi pot aplicar la política de signatura electrònica de l'MMB sempre que es tracti de documents previs, que no han estat creats específicament pel ciutadà per a ser presentats davant l'administració

En qualsevol cas, s'han d'acceptar – i poder validar – les signatures dels documents ofimàtics que es determinin a l'Esquema Nacional d'Interoperabilitat i a l'Esquema Nacional de Seguretat.

S'accepten les còpies digitalitzades dels documents en suport paper, produïdes pels ciutadans. Es recomana protegir aquests documents, en tot cas, amb la signatura electrònica de la sol·licitud (exemple: mitjançant la inclusió dels resums criptogràfics dels documents en el formulari a signar). D'aquesta forma, sempre existeix una prova dels documents que es van lliurar a l'MMB, amb independència de la validesa de la signatura dels documents, o fins i tot de que estiguin signats o no.

4 FORMAT I PERFIL DE LA SIGNATURA

En general, el format de la signatura depèn del format del document a signar (exemple: PDF exigeix signar d'acord amb CMS, ODF exigeix signar d'acord amb una variant d'XML Digital Signature).

L'MMB utilitza de forma indistinta els formats de signatura estàndard disponibles per a les administracions públiques de Catalunya en el catàleg de mecanismes de signatura de l'AOC.

Les signatures dels documents amb rellevància externa han de ser suficientment completes perquè els ciutadans les puguin validar sense mitjans que els resultin especialment costosos o que siguin particularment sofisticats.

5 PROCESSOS EN RELACIÓ A LA SIGNATURA ELECTRÒNICA

S'han d'implantar els següents processos en relació amb la signatura electrònica:

- Procés de creació de la signatura electrònica: Consisteix en la successió de passes necessàries per obtenir una signatura digital per a un tipus de contingut concret. Inclou la possibilitat de seleccionar i visualitzar continguts i atributs de signatura, efectuar fluxos de signatura i veure l'estat d'una signatura realitzada.
- Procés de validació inicial de la signatura electrònica: Consisteix en la successió de passes necessàries per verificar una signatura digital per a un tipus de contingut concret, en el moment de la seva recepció. Es tracta d'una verificació parcial, ja que, normalment, a la recepció d'una signatura electrònica no es pot determinar l'estat actual de revocació d'un certificat (degut a què la informació de revocació es publica amb un dia d'endarreriment). Aquesta verificació no incorpora, per exemple, un segell de data i hora a la signatura. Aquest procés s'ha de basar en l'ús del servei de validació del Consorci AOC.
- Procés de validació definitiva de la signatura electrònica. Consisteix en la successió de passes necessàries per verificar una signatura digital per a un tipus de contingut concret, de forma definitiva. Es tracta d'una verificació definitiva, en un moment en què ja es pot determinar l'estat definitiu de revocació d'un certificat (normalment al menys un dia després de la recepció de la signatura). Aquesta verificació, quan resulta apropiat, incorpora un segell de data i hora a la signatura electrònica, o la completa amb les dades necessàries per gaudir d'evidència electrònica. Aquest procés s'ha de basar en l'ús del servei Validador (PSIS) del Consorci AOC.
- Procés de manteniment de la validesa de la signatura electrònica. Consisteix en la successió de passes necessàries per mantenir al llarg del temps la validesa d'una signatura digital per a un tipus de contingut concret, en el moment de la seva recepció. Es tracta d'un procés d'addició de garanties criptogràfiques addicionals (típicament, informacions addicionals i segells de data i hora) que permeten acreditar la producció d'una signatura en un moment concret del temps, fins i tot en cas de ruptura o obsolescència matemàtica dels algorismes de

signatura electrònica. Aquest procés s'ha de basar en l'ús del servei Validador (PSIS) del Consorci AOC o un altre.

L'MMB disposarà del mitjans tècnics per a l'aplicació de la present política de signatura emprant els serveis subministrats pel Consorci AOC o altres proveïdors homologats