POLÍTICA D'IDENTITAT I SIGNATURA ELECTRÒNIQUES

Setembre 2023

Control documental

Classificació de seguretat :	**Públic**
Entitat de destí:	**AJUNTAMENT DE TARRAGONA**
Versió:	3.0
Data edició:	**10/2023**
Fitxer:	Política d'identitat i signatura electròniques_202309_vDEF.docx
Format:	**Word**
Autors:	Servei d'Arxiu i Documentació

ÍNDEX

1. Introducció, objecte i marc normatiu

L'Ajuntament de Tarragona -d'ara endavant, «Ajuntament» o «institució»- estableix la present Política d'identitat i signatura electròniques -d'ara endavant, «Política»-, que evidencia el seu compromís amb l'establiment de mecanismes d'identificació i signatura electrònica, així com amb la producció de documents electrònics amb plena validesa jurídica dins l'estratègia d'implantació de l'administració digital a la institució.

Aquesta Política regula, dins l'àmbit competencial de l'Ajuntament i d'acord amb allò previst en el Reial Decret 4/2010, de 8 de gener, pel que es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica, i la Resolució de 27 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, pel que s'aprova la Norma Tècnica d'Interoperabilitat de la Política de signatura electrònica i certificats de l'Administració:

- L'abast i àmbit subjectiu d'aplicació d'aquest document.
- Les dades per a la identificació de la Política.
- L'atribució de rols i responsabilitats als diferents actors que han de regir la gestió i desenvolupament d'aquesta.
- Les directrius generals relatives als mecanismes per a acreditar la identitat electrònica a l'Ajuntament.
- La identificació de certificats digitals i altres mecanismes d'identificació emprats i admesos per l'Ajuntament, així com la descripció dels procediments per a la seva obtenció i gestió per part de la institució.
- Els sistemes i formats d'identificació i signatura electrònica admesos.
- Els casos d'ús de la signatura electrònica, que permeten tenir un model de referència dels sistemes de signatura que es poden emprar i admetre en cada cas.
- Les comprovacions automàtiques i manuals que portarà a terme l'Ajuntament quan rebi una signatura electrònica per part de tercers.
- L'estratègia de preservació de documents i signatures electròniques.
- Directrius al respecte del manteniment i desenvolupament de la Política.

En aquest context, l'Ajuntament adopta el present document de Política d'identitat i signatura electròniques per establir la tipologia de certificats digitals i signatures electròniques que utilitza i accepta, tant en relació als seus òrgans i unitats com pel que fa a totes les persones que integren la seva organització i els tercers que s'hi relacionen, així com per determinar els seus usos i procediments, els mètodes d'obtenció, emmagatzematge i preservació a llarg termini per poder garantir l'autenticitat, integritat i conservació dels documents signats digitalment mitjançant les aplicacions corporatives de l'Ajuntament.

La implantació del model de signatura electrònica requereix definir quins certificats digitals s'admetran i per quins usos. Per tant, la present Política inclou una relació dels formats tècnics emprats i els tipus de signatura generats o acceptats per l'Ajuntament.

Addicionalment, aquest document estableix les estratègies que l'Ajuntament implementarà per a la preservació a llarg termini de les signatures electròniques.

A aquest document li resulta d'aplicació la normativa en la matèria que es detalla a continuació o la que la substitueixi en un futur, tant a nivell supranacional, estatal, autonòmic i local, com a nivell d'estàndards internacionals i altres convencions.

Normativa d'àmbit europeu

- Reglament (UE) 910/2014 del Parlament Europeu i del Consell de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per les transaccions electròniques en el mercat interior i pel que es deroga la Directiva 1999/93/CE (Reglament eIDAS d'ara endavant).

- Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril, relatiu a la protecció de les persones físiques en allò que respecta al tractament de dades personals i la lliure circulació d'aquestes dades.

- Decisió d'Execució (UE) 2015/1506 de la Comissió de 8 de setembre de 2015, per la qual s'estableixen les especificacions relatives als formats de les signatures electròniques avançades i els segells avançats que han de reconèixer els organismes del sector públic de conformitat amb els articles 27, apartat 5 i 37, apartat 5, del Reglament anteriorment referenciat.

Normativa d'àmbit estatal

- Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques ("Llei 39/2015" en endavant).

- Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic ("Llei 40/2015" en endavant).
- Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança ("Llei 6/2020" en endavant).
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.
- Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat. ("Esquema Nacional de Seguretat" en endavant)
- Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica.
- Reial Decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics.
- Resolució de 27 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Norma Tècnica d'Interoperabilitat de Política de Signatura i Segell Electrònics i de Certificats de l'Administració.
- Resolució de 19 de juliol de 2011, de la Secretaria d'Estat per a la Funció Pública, per la qual s'aprova la Norma Tècnica d'Interoperabilitat de Document Electrònic.
- Resolució de 14 de juliol de 2017, de la Secretaria General d'Administració Digital, per la qual s'estableixen les condicions d'ús de signatura electrònica no criptogràfica, en les relacions dels interessats amb els òrgans administratius de l'Administració General de l'Estat i els seus organismes públics.

Normativa d'àmbit autonòmic

- Llei 26/2010, de 3 d'agost, de règim jurídic i de les administracions públiques de Catalunya.
- Llei 29/2010, del 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya.

Normativa pròpia de l'Ajuntament de Tarragona

La present Política d'identitat i signatura electròniques complementa i desenvolupa el que ja preveu la normativa de l'Ajuntament que es publica a la seu electrònica en l'àmbit de l'Administració Electrònica.

Estàndards internacionals i altres convencions

La present Política es sotmet a tots els estàndards internacionals i altres convencions que puguin resultar d'aplicació en la definició dels diversos mecanismes electrònics d'acreditació de la identitat i els formats i tipus de signatura i segells electrònics. En especial, aquells que determini la política marc de referència a la que es refereix el següent apartat.

2. Abast i àmbit d'aplicació subjectiu de la Política

En el marc del que disposa l'epígraf II.5.1 de la Norma Tècnica d'Interoperabilitat de Política de signatura i segell electrònics i de certificats de l'administració, de 27 d'octubre de 2016, l'Ajuntament de Tarragona s'acull a la Política de signatura electrònica i de certificats en l'àmbit de l'Administració General de l'Estat, aprovada el 30 de maig de 2012 i publicada mitjançant la Resolució de 29 de novembre de 2012 de la Secretaria d'Estat d'Administracions Públiques o aquella que la substitueixi en un futur, i adopta el present document per a completar aquells sistemes d'identitat i signatura electròniques que empra l'Ajuntament i que la Política marc de referència no contempla.

En aquest sentit, l'Ajuntament de Tarragona aplicarà el mateix *"OID" (Identificador d'objecte)* que la Política marc de referència, ja que tot i que el present document reconegui altres mecanismes d'identificació i signatura, aquests es completaran amb una signatura que farà referència a aquesta.

Per altra banda, aquest document resulta d'aplicació a totes aquelles persones o entitats que estableixin relacions amb l'Ajuntament que requereixin la producció o intercanvi de documents electrònics autèntics.

La Política també s'aplica a totes les persones que integren l'Ajuntament, els seus organismes autònoms i les societats mercantils de capital íntegrament local, amb independència de la modalitat contractual que determini la seva relació amb la institució, la posició jeràrquica que ocupin i sigui quin sigui el centre de treball en el que prestin serveis.

3. Identificació de la Política d'identitat i signatura electròniques de l'Ajuntament de Tarragona

Nom del document	Política d'identitat i signatura electròniques de l'Ajuntament de Tarragona
Versió	1.0
Identificador de la política	OID de la Política de Signatura Electrònica i de Certificats de l'Administració General de l'Estat: 2.16.724.1.3.1.1.2.1.9 a la qual s'adhereix l'Ajuntament de Tarragona.
URL de referència de la política	https://seu.tarragona.cat/
Data i òrgan d'aprovació	Junta de govern local, 17 de novembre de 2023
Àmbit d'aplicació	Documents i expedients produïts i/o custodiats per l'Ajuntament de Tarragona.
Política marc de referència	Política de Firma Electrónica y de Certificados de la Administración General del Estado.[1]
Responsable de la política	Secretaria de l'Ajuntament de Tarragona

[1] https://sede.administracion.gob.es/PAG_Sede/dam/sedePAG/documentos/politica_de_firma_anexo_1.pdf en data d'aprovació de la present política.

4. Rols i Responsabilitats

A continuació, s'estableix l'atribució de rols i responsabilitats dels departaments de l'Ajuntament implicats pel present document:

4.1 Alcaldia

- Desenvolupar, aprovar, publicar i mantenir la present Política i els seus Annexes.
- Proposar l'execució d'auditories per a verificar el compliment de la Política.

4.2 Secretaria

- Garantir la publicació a la seu electrònica de les versions actualitzades de la present Política.
- Gestionar la formació al personal de l'Ajuntament sobre l'ús d'aquesta Política.
- Proposar l'actualització d'aquesta Política a l'òrgan competent.
- A través del Departament d'Ordenació Corporativa, portar a terme el manteniment de l'inventari de certificats digitals de la institució.

4.3 Servei de Tecnologies de la Informació i les Comunicacions

- Implantar i mantenir les plataformes i solucions tecnològiques apropiades per donar compliment a aquesta Política.

4.4 Tots els òrgans i unitats

- Conèixer la Política i complir amb el seu contingut.

5. Identitat electrònica a l'Ajuntament de Tarragona

L'ús de les relacions telemàtiques implica la necessitat d'identificar totes les parts participants de forma segura i certa per evitar el repudi de les comunicacions.

En aquest sentit, a continuació, es recopilen i defineixen els diferents sistemes que l'Ajuntament admet per a l'acreditació electrònica de la identitat de les persones que s'hi relacionen, d'acord amb el marc jurídic vigent:

1. **Certificats digitals qualificats de signatura electrònica avançada o qualificada**, emesos per un prestador inclòs en la llista de prestadors qualificats de serveis electrònics de confiança.

2. **Certificats digitals qualificats de segell electrònic per a actuació administrativa automatitzada**, emesos per un prestador inclòs en la llista de prestadors qualificats de serveis electrònics de confiança.

3. **Identitats digitals basades en sistemes de clau concertada recolzades en un sistema de registre previ**. En aquest sentit, l'Ajuntament podrà usar els sistemes d'identificació basats en registre previ que desenvolupi el propi ens prèvia comunicació a la Secretaria General d'Administració Digital del Ministeri d'Assumptes Econòmics i Transformació Digital o, mitjançant l'adhesió al corresponent conveni, usar els serveis que presta el Consorci Administració Oberta de Catalunya ("Consorci AOC" d'ara endavant) a través del sistema VÀLid o els de l'Administració General de l'Estat com Cl@ve Permanente, Cl@ve PIN24h o Cl@ve Firma.

4. **Sistemes d'identificació biomètrica**, que impliquen que les dades obtingudes es guardin de forma xifrada i que, quan la persona interessada s'hagi d'identificar, es porti a terme la captura de les dades biomètriques per a comparar-les amb les ja emmagatzemades per validar la seva identitat.

L'Ajuntament haurà de donar publicitat, a la seva seu electrònica, als sistemes d'identificació admesos en cada moment.

L'apartat 8 d'aquest document desenvolupa els casos d'ús de cada sistema, determinant l'admissibilitat d'un o altre en funció dels requeriments de seguretat aplicables.

6. Certificats digitals i altres mecanismes de provisió d'identitats digitals a l'Ajuntament

6.1 Certificats digitals utilitzats per l'Ajuntament

Amb l'objectiu de donar compliment a les previsions dels apartats anteriors, l'Ajuntament i el seu personal hauran de fer servir els següents certificats digitals:

- **Certificats de representant.** Certificats qualificats personals dels quals únicament poden disposar les persones que tenen atribuïda la competència de representar l'Ajuntament davant de tercers, que contenen la dada de vinculació amb la institució i són emesos per un prestador inclòs en la llista de prestadors qualificats de serveis electrònics de confiança.

- **Certificats d'empleat públic.** Certificats qualificats personals dels quals pot disposar qualsevol persona física que treballi en el sector públic, que conté la dada de vinculació amb l'ens en què treballa i que és emès per un prestador inclòs en la llista de prestadors qualificats de serveis electrònics de confiança. Aquest tipus de certificat s'estableix com el d'ús habitual per part del personal al servei de l'Ajuntament en el desenvolupament de les seves funcions professionals. En aquest sentit, només permet el seu ús en l'àmbit privat quan no existeixi un risc de confusió sobre la intervenció de l'Ajuntament en l'actuació que requereixi l'ús del certificat.

- **Certificats d'empleat públic amb pseudònim.** Certificats qualificats personals que identifiquen empleats públics de forma anònima a través de l'aplicació d'àlies que, en els termes de l'article 23 del RD 203/2021, només es pot emetre per al seu ús en cas d'actuacions que afectin informació classificada, la seguretat pública, la defensa nacional o altres actuacions per a la realització de les quals estigui legalment justificat l'anonimat emès per un prestador inclòs en la llista de prestadors qualificats de serveis electrònics de confiança.

- **Certificats de pertinença a empresa.** Certificats qualificats personals dels quals poden disposar les persones físiques vinculades a una empresa privada que contenen la dada de vinculació a aquesta en exercici de les seves funcions laborals emesos per un prestador inclòs en la llista de prestadors qualificats de serveis electrònics de confiança.

- **Certificats de segell electrònic.** Certificats que serveixen per autoritzar l'actuació administrativa automatitzada segons l'article 42 de la Llei 40/2015. Cal usar aquest tipus de certificat per realitzar compulses i còpies electròniques, foliat d'expedients i emissió de documents que no requereixin la intervenció d'empleats públics.

- **Certificats de servidor i aplicació.** Certificats que serveixen per a la identificació d'aplicacions, servidors, sistemes o serveis web o per a l'intercanvi de dades entre administracions, administracions i ciutadans i entre administracions i empreses. Aquest tipus de certificat és el requerit per a una aplicació que envia missatges que requereixin assegurar la seva integritat i autenticitat. L'ús d'aquest tipus de certificat no produeix cap efecte jurídic.

- **Certificats de servidor segur.** Certificats que permeten garantir l'accés segur en els entorns de tramitació telemàtica de la institució, com per exemple la seu electrònica o les pàgines web de l'Ajuntament, establint comunicacions xifrades amb els usuaris del servidor web utilitzant la tecnologia SSL o TLS. Es podrà aplicar qualsevol certificat emès per autoritats de certificació amb un alt nivell de reconeixement de les seves claus públiques en els navegadors web d'ús més estès. L'ús d'aquest tipus de certificat no produeix cap efecte jurídic.

L'Ajuntament haurà de donar publicitat, a la seva seu electrònica, als certificats digitals de què disposi en cada moment exceptuant aquells vinculats amb persones físiques.

6.2 Certificats digitals admesos per l'Ajuntament

D'acord amb el que estipulen els articles 9 i 10 de la Llei 39/2015, les persones interessades que es relacionin amb l'Ajuntament podran fer ús dels certificats referenciats en la llista de prestadors de serveis electrònics de confiança que manté el Ministeri competent [2]per identificar-se en les actuacions en les quals intervinguin, així com per a la signatura electrònica de la documentació en suport digital.

Els prestadors i certificats que, malgrat estar en la llista del Ministeri, no estiguin reconeguts en els sistemes que s'utilitzin a l'Ajuntament, no podran ser utilitzats en els tràmits o procediments que impliquin una validació automàtica.

6.3 Certificats digitals del personal de l'Ajuntament

En aquells supòsits en què el personal de l'Ajuntament necessiti disposar de certificat electrònic, podrà usar-ne un d'empleat públic o, quan el càrrec o les tasques i competències del lloc de treball ho requereixin, de representant. Només en casos puntuals i justificats, es permetrà l'ús del certificat digital de persona física per part del personal de l'Ajuntament. Altrament, en el cas de tercers que participin o col·laborin puntualment amb l'Ajuntament, podran usar-ne un de persona física o un de vinculació amb l'Ajuntament. En particular:

- Totes les persones que per càrrec o designació puguin representar l'Ajuntament hauran de tenir com a mínim un certificat electrònic de representant.

- Tot el personal de l'Ajuntament que en l'exercici de les seves funcions necessiti signar documents electrònics o realitzar alguna de les tasques per a les quals es requereix certificat, podrà demanar un certificat de vinculació amb l'Ajuntament d'acord amb el procediment referenciat a l'apartat 6.5.1 de la present Política. És responsabilitat de la persona empleada de l'Ajuntament assegurar-se de la vigència del seu certificat.

- La resta de les persones vinculades a l'Ajuntament o persones que hi participin o hi col·laborin puntualment, podran utilitzar un certificat de persona física o obtenir un certificat

[2] https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx en data d'aprovació de la present política (veure la taula de l'apartat 3).

electrònic de vinculació amb l'Ajuntament, acompanyant la justificació de la seva necessitat verificada pel seu superior jeràrquic o pel responsable del servei amb el qual col·labori.

- En el cas que el personal de l'Ajuntament necessiti, d'acord amb les funcions del seu lloc de treball, tractar informació classificada, realitzar actuacions relacionades amb la seguretat pública o defensa nacional o emprendre altres actuacions que per a la seva realització estigui legalment justificat l'anonimat, podrà usar els certificats d'empleat públic amb pseudònim.

6.4 Supòsits autoritzats per a utilitzar els certificats de signatura electrònica

Els certificats emesos a favor del personal empleat de l'Ajuntament, d'acord amb la seva condició de treballadors de l'Ajuntament, s'emeten per utilitzar-se en els procediments i tràmits que es desenvolupin en el marc de les funcions i activitats de l'Ajuntament. Concretament, per a:

- Autenticar-se en els sistemes d'informació de l'Ajuntament, si correspon.
- Autenticar-se davant els portals de les administracions amb les quals es relacioni l'Ajuntament.
- Signar electrònicament documents generats per l'Ajuntament.
- Signar electrònicament documents generats per un tercer, relacionats amb un procediment o expedient electrònic en l'àmbit de l'Ajuntament.
- De forma puntual i justificada, per a fins personals.

6.5 Procediments relacionats amb el cicle de vida dels certificats digitals

6.5.1 Obtenció, renovació i revocació

La Secretaria de l'Ajuntament establirà els procediments per a l'obtenció, renovació i revocació dels diferents certificats en ús a l'Ajuntament, d'acord amb l'apartat 4.2 de la present Política i les guies desenvolupades per l'entitat prestadora de serveis de certificació de referència a l'Ajuntament, el Consorci AOC.

La renovació dels procediments de l'apartat anterior es farà d'ofici, sempre que els canvis en els aspectes tecnològics o normatius ho facin necessari.

Els procediments vigents en cada moment es faran accessibles a tot el personal en l'àmbit que correspongui dins d'un espai accessible per a tot el personal de la organització.

Com a mínim, caldrà formular procediments per a:

- Obtenir un certificat de representant de l'Ajuntament.
- Obtenir un certificat d'empleat públic vinculat a l'Ajuntament.
- Obtenir un certificat de segell electrònic.
- Revocar un certificat electrònic.
- Renovar un certificat electrònic.

6.5.2 Emmagatzematge dels certificats digitals

Els certificats digitals que s'utilitzin a l'Ajuntament es podran trobar a:

- El repositori de gestió de certificats dels ordinadors dels respectius llocs de treball en els casos de certificats d'empleat públic i de representant, que permeten generar signatures avançades. La persona titular del certificat és responsable de protegir l'ús dels certificats emmagatzemats mitjançant una contrasenya o codi PIN que només ella conegui.
- La targeta criptogràfica, per a certificats d'empleat públic o de representant en suport targeta criptogràfica, que permeten generar una signatura qualificada.
- L'eina programari de gestió centralitzada de certificats que l'Ajuntament determini per emmagatzemar certificats d'empleat públic o de representant basada en un servei al núvol d'emmagatzematge de certificats digitals per part d'una entitat prestadora de serveis de confiança que els faci accessibles de manera segura als usuaris autoritzats dins la xarxa de l'Ajuntament, que permetrà generar signatures qualificades.
- El repositori de gestió de certificats digitals dels servidors de l'Ajuntament o en un servei núvol d'emmagatzematge segur de certificats digitals per part d'una entitat prestadora de serveis de confiança per a certificats de segell electrònic per dur a terme l'actuació administrativa automatitzada, els d'aplicació o per a certificats de servidor web i seu electrònica.

En cas que per la prestació de serveis de seguretat resulti imprescindible, l'Ajuntament podrà proporcionar accés als certificats de segell electrònic a tercers mitjançant l'accés als serveis d'emmagatzematge segurs de certificats al núvol o a través de la instal·lació en els seus propis

servidors per tal que l'Ajuntament pugui executar tasques automàtiques. Aquestes cessions hauran d'estar descrites en un contracte o conveni a celebrar entre l'Ajuntament i el tercer, acotades a usos concrets i subjectes a les potestats de verificació pròpies de l'Ajuntament.

6.5.3 Manteniment de l'inventari de certificats digitals de l'Ajuntament

D'acord amb l'apartat 4.3 del present document, el Departament d'Ordenació Corporativa adscrit a la Secretaria General, de l'Ajuntament durà a terme el manteniment de l'inventari de certificats digitals de la institució. Aquest inventari serà únic per a tots els certificats personals sense distinció de l'entitat certificadora que els emeti i inclouran la informació necessària per a la gestió d'aquests, que contindrà, com a mínim:

- La titularitat del certificat.
- L'autoritat emissora.
- La tipologia de certificat.
- La data de caducitat.

Es revisarà, de forma proactiva, la vigència dels diferents certificats digitals amb una periodicitat mínima semestral. Aquesta revisió podrà comportar la revocació de certificats digitals que ja no siguin conformes amb la present Política i les seves successives modificacions.

Els principals motius que poden comportar la revocació dels certificats són:

- Que les dades que conté el certificat ja no siguin certes.
- Que la persona ja no ostenti el càrrec que identifica el certificat o no tingui atribuïdes les mateixes competències que en el moment de la seva emissió.
- Que la seguretat del certificat hagi estat compromesa.

Pel que fa a les polítiques d'emissió, gestió i vigència dels certificats, s'haurà d'estar al cas del que estableixen les autoritats de certificació responsables.

7. Sistemes de signatura electrònica

Els sistemes de signatura electrònica desenvolupats en el present apartat complementen el que disposa la Política de signatura electrònica i de certificats en l'àmbit de l'Administració General de

l'Estat i son els que es podran usar en les aplicacions corporatives de l'Ajuntament amb la finalitat de garantir l'autenticitat, integritat, inalterabilitat i conservació dels documents signats digitalment.

En aquest sentit, la present Política defineix l'ús d'un conjunt de sistemes de signatura electrònica i els seus corresponents casos d'ús continguts en l'apartat 8 destinats a facilitar la presa de decisions al respecte de quin sistema de signatura electrònica emprar en cada cas concret.

Quan els empleats de l'Ajuntament participin en procediments definits per una altra organització, generaran les signatures en els formats que aquesta organització determini; i, si cal afegir còpia a un expedient de l'Ajuntament, s'aplicaran les comprovacions indicades a l'apartat 9 d'aquesta Política.

En tot cas, l'Ajuntament de Tarragona haurà de donar publicitat, a la seva seu electrònica, als sistemes de signatura electrònica admesos en cada moment

A continuació es classifiquen els sistemes de signatura electrònica en funció de si requereixen intervenció humana o si son plenament automatitzats:

7.1 Sistemes de signatura que requereixen intervenció humana

a. Signatura electrònica mitjançant certificat digital personal

Consisteix en el sistema de signatura electrònica en el qual, partint de la clau privada del certificat d'una persona, es xifra el resum criptogràfic del document a signar i s'incorpora informació del certificat usat per efectuar la signatura, per exemple, la data de signatura o referència a la Política de signatura i certificats de l'AGE a la que s'adhereix l'Ajuntament de Tarragona.

L'Ajuntament farà servir aquest sistema per signar documents electrònics per part del personal de l'Ajuntament i admetrà documents electrònics signats amb aquest sistema per part de tercers que s'hi relacionin.

b. Signatura electrònica basada en claus concertades més les evidències de voluntat de signatura

L'ús d'aquest sistema d'identificació més signatura basat en claus concertades apareix regulat a l'article 10.2.c) de la Llei 39/2015 i permet generar signatures electròniques a partir de l'acreditació de la identitat de la persona signant juntament amb la seva voluntat de signatura. D'acord amb la mateixa llei, caldrà comunicar el desenvolupament d'aquests sistemes a la Secretaria General d'Administració Digital adscrita al Ministeri corresponent del Govern estatal i adjuntar una declaració responsable conforme es compleixen tots els requisits establerts en

la normativa vigent. En tot cas, hauran de transcórrer dos mesos des de la referenciada comunicació per a que aquests sistemes puguin produir efectes jurídics.

En aquest sentit, el sistema de signatura es basa en la identificació d'una persona a través de l'aportació del seu usuari i contrasenya com a primera evidència d'autenticació complementada amb la captura de dades de context en el moment de la signatura, amb un element criptogràfic addicional de garantia de la integritat. La parella de claus concertades haurà estat proporcionada prèviament per l'Ajuntament d'acord amb els protocols establerts.

La usabilitat d'aquesta modalitat de signatura està condicionada per la qualitat del mecanisme de distribució de les identitats. Així doncs, els procediments d'obtenció de les credencials que es puguin fer servir per a generar aquests tipus de signatures hauran de garantir:

- Previ a l'entrega de les credencials, la identitat de la persona ha d'haver estat verificada certament per part de l'Ajuntament. Si no es compleix aquesta condició, no es podrà fer servir la parella de claus per a generar signatures i el sistema de gestió de credencials haurà de tenir la capacitat de deixar constància d'aquesta circumstància. Una verificació posterior de la identitat permetrà convalidar les credencials per al seu ús futur com a mecanisme de signatura.

- Els sistemes de gestió de les credencials han de garantir la seva custòdia segura, la seva renovació amb una periodicitat conforme a les Polítiques de Seguretat de l'Ajuntament i un control sobre el nombre d'intents fallits que provoquin el bloqueig de la credencial per a prevenir un ús fraudulent.

- Els usuaris hauran de rebre informació oportuna sobre la criticitat d'aquest sistema de credencials i la importància de garantir la seva confidencialitat.

Les aplicacions que utilitzin aquest sistema de signatura hauran de permetre que la persona usuària verifiqui les dades a signar mitjançant la inclusió de frases que manifestin la voluntat de signatura de forma inequívoca, com, per exemple, mitjançant la confirmació del botó de l'aplicació corresponent amb una expressió clara del document o contingut que es pretengui signar. Addicionalment, es sol·licitarà que la persona usuària es torni a identificar amb la finalitat de garantir el no repudi de la signatura.

Com a mesura addicional per garantir la robustesa de la identificació, es pot requerir addicionalment a l'usuari la resposta a un repte d'identificació basat en l'enviament d'un codi d'un sol ús a una adreça de correu electrònic o un dispositiu mòbil registrat prèviament. Aquesta mesura es considera complementària a la de la parella de claus, constituint un doble factor d'identificació.

Un cop verificada la identitat, es crearà un fitxer d'evidències que s'emmagatzemarà per consolidar la signatura.

Les evidències a capturar en aquest sistema de signatura hauran d'incloure, com a mínim:

- Nom, cognoms, compte d'usuari i codi identificador de la persona signant.
- Data i hora de la identificació de la persona signant en l'aplicació.
- Identificador del tràmit.
- Identificador de la transacció de signatura i l'aplicació responsable de la transacció de signatura.
- Data i hora de la transacció de signatura.
- Títol i resum digital o "hash" de les dades signades.
- Dades de navegació: direcció IP de l'usuari i navegador emprat.

La validesa jurídica del sistema de signatura electrònica efectuada mitjançant claus concertades juntament amb les evidències de la voluntat de signatura està vinculada al document electrònic i a les evidències del procés d'identificació de la persona signant que accepta la signatura.

És possible que el document electrònic inclogui més d'una signatura electrònica basada en claus concertades juntament amb les evidències de la voluntat de signatura. En qualsevol cas, s'haurà de poder garantir la possibilitat de verificar l'autenticitat de cadascuna d'elles.

En el cas de conflicte entre les signatures que incorporin el document electrònic, l'Ajuntament podrà acreditar:

- Que el procediment de signatura està regulat de forma específica.
- Que s'han generat les evidències en totes les signatures de la mateixa tipologia.
- Que la signatura es va produir en un moment determinat mitjançant l'aplicació d'un segell de temps.
- Que el document electrònic no ha estat modificat mitjançant la aplicació del "hash" en les evidències del document.

- Que s'ha aplicat una signatura secundària al document electrònic consistent en l'aplicació d'un certificat de segell electrònic de l'Ajuntament que dona garantia a la integritat del conjunt.

L'Ajuntament podrà usar altres sistemes de signatura electrònica basats en claus concertades més les evidències de voluntat de signatura com el sistema idCAT-SMS del Consorci AOC regulat per l'ACORD GOV/92/2015, de 16 de juny o el sistema Cl@ve de l'Administració General de l'Estat regulat en la Resolució de 14 de desembre de 2015, de la Direcció de Tecnologies de la Informació i Comunicacions. En aquests casos, els sistemes de signatura hauran d'haver estat comunicats a la secretaria del Ministeri corresponent d'acord amb l'indicat a l'article 10.2.c de la Llei 39/2015. En aquests casos, les evidències que capturarà el sistema les determinarà l'entitat desenvolupadora del sistema.

c. Signatura electrònica del personal de l'Ajuntament basada en un sistema d'identificació completat amb Codi Segur de Verificació (CSV)

L'Ajuntament pot usar, per a la producció de signatures electròniques del seu personal, un sistema basat en la identificació de les persones signants completat amb Codi Segur de Verificació (CSV).

L'ús d'aquest sistema d'identificació més signatura basat en claus concertades apareix regulat a l'article 10.2.c) de la Llei 39/2015 i permet generar signatures electròniques a partir de l'acreditació de la identitat de la persona signant juntament amb la seva voluntat de signatura. D'acord amb la mateixa llei, caldrà comunicar el desenvolupament d'aquests sistemes a la Secretaria General d'Administració Digital adscrita al Ministeri corresponent del Govern estatal i adjuntar una declaració responsable conforme es compleixen tots els requisits establerts en la normativa vigent. En tot cas, hauran de transcórrer dos mesos des de la referenciada comunicació per a que aquests sistemes puguin produir efectes jurídics.

Concretament, l'ús d'aquest sistema de signatura electrònica està reservat únicament al personal de l'Ajuntament i es basa en la prèvia identificació de la persona signant mitjançant una de les identitats digitals en ús per part de l'Ajuntament d'acord amb l'apartat 5 d'aquesta Política.

Només si la persona usuària s'identifica correctament mitjançant aquest mecanisme de signatura es generarà un CSV vinculat unívocament al document, que s'incorporarà al document signat juntament amb una menció relativa al valor original del document i la seva vinculació amb la persona signant.

La validesa jurídica del sistema de signatura electrònica efectuada mitjançant l'ús de sistemes d'identitat digital està vinculada al document electrònic i a les evidències del procés

d'identificació de la persona signant que accepta la signatura i que quedarà regulat per la Política de Seguretat de la Informació de l'Ajuntament.

Les aplicacions que utilitzin aquest sistema de signatura hauran de permetre que la persona usuària verifiqui les dades a signar mitjançant la inclusió de frases que manifestin la voluntat de signatura de forma inequívoca, com, per exemple, mitjançant la confirmació del botó de l'aplicació corresponent amb una expressió clara del document o contingut que sigui objecte de signatura.

Per a fer-ho, se sol·licitarà l'autenticació de la persona usuària en el moment de procedir a la signatura amb la finalitat de garantir el no repudi d'aquesta.

Un cop verificada la identitat, es crearà un fitxer d'evidències que s'emmagatzemarà en el mateix document electrònic. En el cas en que no fos tècnicament possible, les evidències es desaran en els sistemes corporatius de l'Ajuntament identificant-se formalment el lloc concret en el que es desen en el procediment administratiu que reguli el procediment de signatura.

Posteriorment a la incorporació de les evidències, es procedirà a signar el document electrònic a partir de l'aplicació d'un CSV.

Les evidències objecte de captura hauran d'incloure, com a mínim:

- Nom, cognoms, compte de persona usuària i codi identificador (NIF o similar) de la persona signant.
- Data i hora de la identificació de la persona signant en l'aplicació.
- Identificador del tràmit.
- Identificador de la transacció de signatura i l'aplicació responsable de la transacció de signatura.
- Data i hora de la transacció de signatura.
- Resum digital o "hash" de les dades signades.
- Dades de navegació: direcció IP del client i navegador utilitzat.
- Vincle amb el CSV generat.

Aquest sistema podrà ser emprat per a qualsevol acte resolutori o de tràmit que requereixi la seva signatura per part del personal de l'Ajuntament. Els documents que es signin mitjançant

el present sistema no requeriran la incorporació de signatura electrònica basada en certificats digitals.

La validesa jurídica del sistema de signatura electrònica efectuada mitjançant claus concertades més evidències de la voluntat de signatura està vinculada al document electrònic i a les evidències del procés d'identificació de la persona signant que accepta la signatura.

No és possible, en aquest cas, que el document electrònic contingui més d'una signatura electrònica basada en claus concertades més les evidències de voluntat de signatura.

En el cas en que es produeixi conflicte entre les signatures que incorporin el document electrònic, l'Ajuntament podrà acreditar:

- Que el procediment de signatura està regulat de forma específica.
- Que s'han generat les evidències en totes les signatures de la mateixa tipologia.
- Que el document no s'hagi modificat mitjançant l'aplicació del "hash" en les evidències del document.

En les comunicacions de documents electrònics a altres òrgans, organismes o entitats fora de l'abast de l'Ajuntament i sempre que ho determinin les parts implicades, la interoperabilitat dels documents signats amb CSV es garantirà mitjançant la superposició d'un segell electrònic com a mecanisme de verificació automàtica de l'origen i integritat dels documents electrònics.

d. Signatura electrònica basada en sistemes d'identificació completats amb un segon factor d'autenticació

L'ús del sistema de signatura electrònica basat en sistemes d'identificació basats en claus concertades consisteix, per la seva naturalesa descrita en els apartats anteriors, en un mètode de signatura electrònica relativament simple. Per aquest mateix motiu, es recomana afegir un complement de segon factor d'autenticació basat en un dels sistemes següents:

- Sistemes "One-Time Password" (OTP), que permeten la confirmació de la identitat de la persona signant mitjançant l'enviament d'una contrasenya d'un sol ús proporcionada via missatge de text (SMS) al telèfon o adreça de correu electrònic que hagi estat registrat prèviament a nom d'aquesta persona a l'Ajuntament. Per tant, no serà possible utilitzar aquest mecanisme si l'Ajuntament, prèviament al moment de la signatura, no disposa d'una adreça de correu electrònic o del número de telèfon de la persona signant, o si aquestes dades es proporcionen en el mateix moment de la signatura.

- Sistemes d'aplicacions residents de gestió d'identitats que permeten la confirmació de la identitat de la persona signant mitjançant la generació de codis d'autenticació amb contrasenya d'un sol ús en sistemes instal·lats en els dispositius de les persones signants, com el sistema "Google Authenticator" o "Microsoft Authenticator".

Durant el procés de la signatura, l'usuari haurà superat els reptes d'identitat mitjançant la recepció del correu electrònic a l'adreça abans esmentada o donant resposta a un repte d'identificació basat en missatge de text. Si aquest sistema és completat amb una identificació de l'usuari en l'aplicació mitjançant credencial de claus concertades, la combinació d'ambdós mecanismes constitueix, per tant, un doble factor d'autenticació.

La validesa jurídica del sistema de signatura electrònica efectuada mitjançant l'ús de sistemes de doble factor d'autenticació està vinculada al document electrònic i a les evidències del procés d'identificació de la persona signant que accepta la signatura i quedarà regulat per la Política de Seguretat de la Informació de l'Ajuntament.

Es demanarà l'autenticació de la persona usuària en el moment de procedir a la signatura amb la finalitat de garantir el no repudi de la mateixa.

Un cop verificada la identitat, es crearà un fitxer d'evidències i aquestes s'emmagatzemaran en el mateix document electrònic. En el cas que no fos tècnicament possible emmagatzemar aquest fitxer d'evidències en el mateix moment, les evidències es guardaran en els sistemes corporatius de l'Ajuntament, identificant-se formalment el lloc concret en el qual s'emmagatzemaran en el procediment administratiu que reguli el procediment de signatura.

Posteriorment a la incorporació de les evidències, es procedirà a signar el document electrònic, o el paquet d'evidències si aquestes no s'han pogut consolidar, mitjançant l'ús d'un certificat digital de segell electrònic de l'Ajuntament i completat amb un segell de temps, en qualsevol cas, segells emesos per prestadors de serveis de confiança.

Les evidències objecte de captura hauran d'incloure, com a mínim:

- Nom, cognoms, compte d'usuari i codi identificador (NIF o similar) de la persona signant.
- Títol i resum criptogràfic o "hash" del document signat.
- Data i hora de la transacció de signatura.
- Forma d'identificació de la persona signant (nom d'usuari o identitat al·legada).
- En el cas de l'ús de sistemes OTP, correu electrònic o número de telèfon al qual s'ha manat el repte addicional emès.

- En el cas de l'ús de sistemes d'aplicacions residents de gestió d'identitats, adreça MAC d'identificació del dispositiu, codi introduït per identificar l'usuari o identificador propi de l'aplicació que identifiqui la seva instal·lació en el dispositiu concret.
- Verificació que el repte ha estat superat amb èxit.
- Identificador de la transacció de signatura i l'aplicació responsable o sistema de tramitació que gestiona la signatura.
- Dades de navegació: IP des de la que es connecta la persona usuària i navegador utilitzat.
- En el cas de conflicte entre les signatures que incorpori el document electrònic, l'Ajuntament podrà acreditar:
- Que el procediment de signatura està regulat de forma específica.
- Que s'han generat les evidències en totes les firmes de qualsevol tipus.
- Que la signatura es va produir en un moment determinat mitjançant l'aplicació del segell de temps.
- Que el document no ha estat modificat mitjançant l'aplicació del "hash" en les evidències del document.
- Que s'ha aplicat una signatura secundària al document electrònic consistent en l'aplicació d'un certificat de segell electrònic de l'Ajuntament.

e. Signatura electrònica biomètrica

Aquest sistema de signatura electrònica avançada es genera a partir de les dades biomètriques de la persona signant, que s'incorporen, de forma xifrada, al resum criptogràfic dels documents electrònics generats, de manera que permeten acreditar l'auditoria de la signatura aplicada mitjançant la informació necessària següent:

- Dades biomètriques de la persona que signa el document de forma manuscrita que es recullen mitjançant elements específics de captura que permeten la visualització del document en el mateix acte de signatura, entre ells:
- El detall temporal concretat a l'inici, final i durada en mil·lisegons del procés de signatura del document.

- El detall del traçat, en relació amb la velocitat, acceleració i pressió d'aquest en tota la seva figura.

- Altra informació que pugui resultar rellevant per al procés de signatura d'acord amb les normes ISO 19794-7:2014 i ISO/IEC 19794-7:2021.

Aquest sistema de signatura electrònica avançada només s'aplica en la biometria de la signatura manuscrita, sense usar altres mesures biomètriques com el reconeixement facial o l'ús de l'empremta dactilar que queden fora de l'àmbit d'aquesta Política, sense perjudici que es puguin considerar en un futur.

El xifrat de la informació es duu a terme mitjançant la clau pública d'un certificat específic de signatura electrònica biomètrica que s'emmagatzema en els servidors de l'Ajuntament. La clau privada la custodiarà la Secretaria de l'Ajuntament o un tercer de confiança a qui se li podrà requerir quan sigui necessari perquè verifiqui les signatures biomètriques en cas de reclamació o litigi.

Un mateix document podrà incloure més d'una signatura biomètrica, però sempre de forma paral·lela entre elles.

Un cop s'hagin realitzat totes les signatures biomètriques en paral·lel i s'hagi xifrat la informació detallada al principi d'aquest apartat, aquesta es guardarà de forma conjunta amb el document i, amb l'objectiu de garantir la integritat d'aquest últim, es realitzarà, sobre aquest, una signatura electrònica automàtica de segell electrònic d'aplicació pertanyent a l'Ajuntament completada amb un segell de temps.

En conseqüència, la validesa jurídica de la signatura electrònica biomètrica estarà vinculada al document i a les evidències biomètriques que es guarden dins d'aquest mateix de forma xifrada amb l'aportació de la signatura electrònica i el segell de temps per evidenciar la seva integritat.

En cas de conflicte, una vegada desxifrades les dades per part de la Secretaria de l'Ajuntament o del tercer de confiança que custodia la clau privada del certificat de xifrat, s'haurà de demanar un peritatge de les dades biomètriques guardades en el document i acarar-les amb una nova presa en condicions similars, pel que fa a la maquinària, aplicacions i programes usats en la signatura controvertida, de dades biomètriques de la persona a qui s'al·lega que pertanyen.

f. Signatura de nivell alt d'acord amb l'Esquema Nacional de Seguretat

D'acord amb els requisits de la signatura electrònica establerts per l'Esquema Nacional de Seguretat (ENS en endavant), aquesta Política reconeix un sistema de signatura electrònica de nivell alt per aquells serveis i actius d'informació que siguin categoritzats com de nivell alt,

segons la categorització de sistemes d'informació i la corresponent declaració d'aplicabilitat de mesures de seguretat de l'ENS portat a terme per l'Ajuntament.

En el cas en que l'Ajuntament requereixi signar un document de nivell alt de seguretat, el sistema de signatura haurà de ser, d'acord amb l'ENS, o bé signatura electrònica qualificada basada en certificat digital qualificat associat a la persona que porta a terme l'acte, utilitzant productes certificats d'acord amb el que estipula l'epígraf 4.1.5 de l'Annex II de l'ENS, o bé emprant la signatura electrònica avançada basada en certificat digital qualificat associat a la persona que realitza l'acte, complementada amb una verificació de la identitat mitjançant claus concertades, tal i com es descriu en l'apartat 7.1.b de la present Política.

Per tant, el certificat digital a aplicar en aquest segon tipus de signatures podrà haver estat emès en suport software, però la plataforma on es trobarà el document electrònic a signar haurà d'incorporar un control d'accés amb usuari i contrasenya o clau d'un sol ús (OTP), i conservar les evidències d'aquesta autenticació en el document electrònic signat o vinculades a aquest.

Aquest sistema de signatura compleix amb el Reforç R4 previst en l'epígraf 5.7.3 de l'Annex II de l'ENS i, per tant, pot aplicar-se a qualsevol tipus de document electrònic, inclús aquells que tinguin riscos de nivell alt associats a la seva autenticitat o integritat. Als efectes que interessen a l'Ajuntament de Tarragona, aquesta signatura avançada completada amb un reforç aporta una garantia d'autenticitat i no repudi comparable a la de la signatura qualificada. La signatura qualificada es podrà seguir utilitzant, però no serà la única solució disponible per a signar els documents de nivell més alt segons l'ENS.

Quan una persona usuària de l'Ajuntament de Tarragona accedeixi al sistema que s'utilitzi per a la tramitació dels documents electrònics o l'emissió de les signatures electròniques, s'identificarà amb credencials concertades (usuari i contrasenya). Un cop autenticat, podrà consultar la documentació i signar la que li correspongui utilitzant el certificat digital qualificat, del qual podrà disposar tant en format de targeta criptogràfica com en suport software instal·lat en el seu ordinador corporatiu.

El sistema de tramitació desarà, de forma sistemàtica, juntament amb el document signat, la informació del registre d'autoria amb tots els processos en la tramitació del document electrònic. Aquest paquet de dades inclou la informació de quan i com la persona usuària es va autenticar en el sistema que li va permetre signar el document. Aquesta evidència, juntament amb el segell de temps que s'afegirà posteriorment a la signatura, serà suficient per a donar compliment al requisit R4 de l'ENS mencionat anteriorment, sempre que es compleixin les següents condicions:

- La identificació de la persona usuària s'ha d'haver produït amb una credencial diferent del propi certificat digital amb el que ha signat.

- L'evidència d'identificació es desa com a complement de seguretat de la signatura, però la pròpia signatura és la que genera el certificat, sense que sigui estrictament necessari que inclogui l'evidència del segon factor d'autenticació.

- S'ha de desar el registre d'auditoria de les identificacions en tots els casos en els que els documents requereixin un sistema de signatura de nivell alt.

7.2 Sistemes de signatura plenament automatitzada

a. Signatura electrònica mitjançant segell electrònic per actuació administrativa automatitzada

Aquest sistema de signatura permet la signatura de documents electrònics de l'Ajuntament mitjançant processos automatitzats sense intervenció directa del personal al seu servei.

Consisteix en un sistema en què, partint de la clau privada d'un certificat digital de segell electrònic, es xifra el resum criptogràfic del document a signar i se li afegeix informació del certificat de segell electrònic usat per efectuar la signatura, per exemple, la data de signatura o referència a la Política d'identitat i signatura electrònica.

Aquest tipus de signatura es podrà utilitzar en les actuacions administratives automatitzades prèviament establertes per l'òrgan competent de l'Ajuntament i publicades a la seu electrònica de la institució, d'acord amb l'article 41.2 de la Llei 40/2015.

b. Signatura electrònica basada en un Codi Segur de Verificació per actuació administrativa automatitzada

L'ús del Codi Segur de Verificació (CSV) vinculat a l'administració pública, òrgan, organisme públic o entitat de dret públic com a mitjà de signatura electrònica està regulat en l'article 42.b) de la Llei 40/2015 i permet comprovar la integritat del document electrònic mitjançant l'accés a la seu electrònica de l'entitat emissora d'aquest.

D'acord amb l'article 41.2 de la Llei referenciada en el paràgraf anterior, l'ús del CSV en els casos d'actuació administrativa automatitzada haurà d'estar previst en la resolució administrativa que autoritzi l'automatització del procediment corresponent.

En conseqüència, el sistema de signatura electrònica basada en un CSV podrà usar-se en les actuacions administratives automatitzades que es determinin mitjançant aprovació per part de l'òrgan competent de l'Ajuntament.

En les comunicacions de documents electrònics a altres òrgans, organismes o entitats fora de l'abast de l'Ajuntament i sempre que ho determinin les parts implicades, la interoperabilitat dels documents signats amb CSV es garantirà mitjançant la superposició d'un segell electrònic com a mecanisme de verificació automàtica de l'origen i integritat dels documents electrònics.

c. Segell de temps

El segell de temps és un tipus de signatura electrònica generada per un tercer de confiança en base a un certificat digital especialment dissenyat a tal efecte que permet acreditar la data i hora en què s'ha produït l'acte. Aquest acte pot fer referència a:

- **El moment de signatura del document.** En aquest cas el segell de temps estarà associat a la signatura electrònica aplicada.
- **El moment de la creació del document.** En aquest altre cas el segell de temps estarà associat al document electrònic.

Aquest tipus de signatura electrònica segella la data i hora de l'instant en què es realitza l'acte mitjançant un segell de temps proporcionat per un prestador de serveis de confiança.

Es podrà disposar d'un proveïdor de segellament de temps alternatiu per garantir la disponibilitat dels procediments de segellament de temps, que haurà d'estar sincronitzat amb fonts fiables de temps.

El procediment d'ús del segell de temps consisteix en la creació d'una evidència sobre una signatura electrònica mitjançant el càlcul del resum criptogràfic del document i/o de les signatures electròniques en cas de ressegellat. És a dir, es realitza una operació matemàtica que s'aplica al conjunt d'informació sobre la qual s'emetrà el segell de temps que resulta en una cadena de bits anomenada "hash" i que es xifra amb la clau privada del certificat de segell de temps usat per a tal operació.

El resultat de l'aplicació del certificat de segell de temps dona com a resultat la incorporació de la data i hora de l'operació en el document electrònic, així com informació del certificat de segell de temps usat per a la seva signatura.

7.3 Sistemes de signatura mixtes

a. Signatura múltiple

El cas de la signatura múltiple es dona quan existeixen dues o més signatures electròniques en el mateix document. Depenent de la forma en què s'han efectuat, es considera que s'han realitzat de forma seqüencial o paral·lela:

- **Signatura seqüencial:** Quan la segona signatura es realitza sobre l'objecte digital ja signat anteriorment. Sempre que sigui possible s'evitarà el seu ús per als circuits de signatura en els quals els documents electrònics s'hagin de signar alhora amb el mateix objectiu per part d'una pluralitat de persones.

- **Signatura paral·lela:** Quan les firmes es refereixen al mateix objecte digital que té un únic resum criptogràfic, sigui perquè s'han generat en format "detached" (separat) o perquè el document està preparat per rebre signatures "attached" (adjuntes) en paral·lel.

L'ús de la signatura múltiple es donarà en diverses actuacions en el marc dels diversos procediments administratius de l'Ajuntament, com ara la signatura de documents electrònics per part de més d'una persona o el ressegellat de documents signats amb caràcter previ a què es pugui posar en dubte la validesa criptogràfica de la signatura electrònica, amb l'objectiu d'actualitzar la seva validesa legal al llarg del temps.

Es procurarà que en tots els casos de signatura de documents electrònics per part de més d'una persona s'utilitzin tecnologies similars, evitant particularment que es generin documents signats d'una banda basant-se en certificats i una altra mitjançant l'ús de la signatura biomètrica.

La combinació de diversos sistemes de signatura electrònica serà possible en els següents casos:

- Signatures electròniques mitjançant l'ús de certificats digitals de forma paral·lela o seqüencial per a qualsevol document electrònic que requereixi més d'una signatura.

- Signatures electròniques mitjançant sistemes basats en claus concertades, de forma paral·lela o seqüencial, en el cas de documents electrònics que requereixin més d'una signatura.

- Signatures electròniques biomètriques, que seran de forma seqüencial, per a documents electrònics que es generin presencialment davant de tercers i requereixin dues o més signatures.

- Signatura electrònica mitjançant un sistema basat en claus concertades i, posteriorment, l'aplicació d'una signatura electrònica mitjançant un certificat digital, de forma paral·lela o seqüencial, per a aquells documents electrònics que requereixin la signatura de dues persones, només una de les quals compta amb certificat electrònic.

Quan concorrin dos sistemes de signatura diferents és important assegurar-se que es conserven correctament les evidències de la signatura no criptogràfica i que el segell electrònic o la signatura digital que s'incorpora en darrer lloc doni cobertura a tot el contingut del document.

8. Casos d'ús de la signatura electrònica

A continuació, es presenten diversos casos d'ús dels sistemes de signatura electrònica descrits a l'apartat 7, caracteritzant-los jurídicament, recomanant l'ús d'un o altre en funció del cas analitzat i determinant els seus requisits de seguretat.

8.1 Signatura electrònica d'un document intern

Aquest cas d'ús fa referència als documents produïts internament per l'Ajuntament, signats per una persona membre de la institució en exercici de les seves funcions o per part de tercers que participin o col·laborin puntualment amb l'Ajuntament, que tinguin com a destinatari un altre usuari intern o el simple compliment d'un pas més en el procediment. En cap cas aplica a documents que hagin de produir efectes jurídics davant de tercers.

En aquest cas es permetrà aplicar la signatura electrònica en documents electrònics en qualsevol moment del seu cicle de vida.

Les seves principals característiques són:

- La signatura electrònica es realitza sobre un document original en suport electrònic.
- El document original i les signatures s'han d'incorporar al sistema en el que es produeixi la signatura.
- La signatura electrònica haurà de ser validada mitjançant un servei o autoritat de validació amb la finalitat d'assegurar la seva integritat i autenticitat.
- Sempre que sigui necessària la preservació del document electrònic al llarg del temps, aquest haurà d'estar en qualsevol dels formats admesos per l'Ajuntament, preferiblement en PDF/A i XML.

En relació amb els tipus de signatura aplicables a aquest cas, s'estableixen els següents requeriments:

Classes de signatura	• Avançada o Qualificada, d'acord amb allò descrit a l'apartat 7.1.a
Tipus de certificat	• Certificat d'empleat públic. • Certificat de representant.
Formats acceptats	• "PAdES-LTV" amb segell de temps o "XAdES-B-T" (d'acord amb el que determini la Política de signatura i certificats de l'AGE vigent).
Nivell de signatura	• Simple, Múltiple (seqüencial o paral·lela).
Aplicació de segell de temps	

8.2 Signatura electrònica d'un document amb valor per tercers

Aquest cas d'ús es refereix a documents produïts internament a l'Ajuntament que han d'estar signats per una persona membre de la institució, o per tercers que col·laborin puntualment amb l'Ajuntament que generen drets i/o obligacions a tercers.

Es permetrà aplicar la signatura electrònica en documents electrònics en qualsevol moment del seu cicle de vida.

Les seves principals característiques són:

- La signatura electrònica es realitza sobre un document original en suport electrònic.
- El document original i les signatures s'han d'incorporar al sistema en el que es produeixi la signatura.

- La signatura electrònica haurà de ser validada mitjançant un servei o autoritat de validació amb la finalitat d'assegurar la seva integritat i autenticitat.

- El document electrònic haurà d'estar en qualsevol dels formats admesos per l'Ajuntament, preferiblement en PDF/A i XML, amb l'objectiu de garantir la seva preservació al llarg del temps.

- S'expedirà una còpia autèntica del document electrònic que ocultarà les dades del DNI de la persona signant, per garantir la protecció de les seves dades personals i s'afegirà un CSV. Aquesta serà la còpia que es facilitarà a tercers.

En relació amb els tipus de signatura aplicables a aquest cas, s'estableixen els següents requeriments:

Classes de signatura	• Avançada o Qualificada, d'acord amb allò descrit a l'apartat 7.1.a
Tipus de certificat	• Certificat de persona física • Certificat d'empleat públic • Certificats de pertinença a empresa • Certificat de representant
Formats acceptats	• "PAdES-LTV" amb segell de temps o "XAdES-B-T" (d'acord amb el que determini la Política de signatura i certificats de l'AGE vigent).
Nivell de signatura	• Simple, Múltiple (seqüencial o paral·lela).
Aplicació de segell de temps	

8.3 Signatura electrònica de documents per part de tercers

Aquest cas d'ús fa referència a aquells documents electrònics produïts per l'Ajuntament o tercers que són signats per aquests últims en un entorn controlat per l'Ajuntament. En el cas que aquest

tipus de documents electrònics se signin en entorns fora del control de l'Ajuntament caldrà atenir-se al que es determina a l'apartat 9 de la present Política.

Concretament, aquest cas aplica en la signatura de documents en el moment de la seva presentació davant d'un registre electrònic, o quan el tercer ha de signar documents electrònics en moments posteriors en la seva participació en un procediment administratiu de l'Ajuntament. En el cas en que la persona signant intervé representada per un tercer, l'Ajuntament haurà de tenir evidències suficients de la capacitat de representació del signatari respecte al tercer.

Les seves principals característiques son:

- La signatura electrònica es realitza sobre un document original en suport electrònic.
- El document original i les signatures s'han d'incorporar al sistema en el que es produeixi la signatura.
- La signatura electrònica haurà de ser validada mitjançant un servei o autoritat de validació amb la finalitat d'assegurar la seva integritat i autenticitat.
- Sempre que sigui necessària la preservació del document electrònic al llarg del temps, aquest haurà d'estar en qualsevol dels formats admesos per l'Ajuntament, preferiblement en PDF/A i XML.

En relació amb els tipus de signatura aplicables a aquest cas, s'estableixen els següents requeriments:

Classes de signatura	• Avançada, d'acord amb allò descrit a l'apartat 7.1.a • Signatura basada en claus concertades amb complement de segon factor d'autenticació, d'acord amb el descrit a l'apartat 7.1.b i 7.1.d d'aquesta Política. • Signatura electrònica biomètrica, d'acord amb el que descriu l'apartat 7.1.e només per part del tercer.
Tipus de certificat	• Per a les signatures generades per tercers amb certificat electrònic serà vàlid qualsevol certificat de signatura definit a l'apartat 6. • Per a la resta dels mecanismes de signatura, certificat de segell electrònic.

Formats acceptats	• "PAdES-LTV" amb segell de temps o "XAdES-B-T" (d'acord amb el que determini la Política de signatura i certificats de l'AGE vigent).
Nivell de signatura	• Simple.
Aplicació de segell de temps	

8.4 Signatura electrònica de contractes, convenis o acords amb altres parts

Aquest cas d'ús aplica als documents de caràcter contractual multilaterals en els quals participa l'Ajuntament de forma conjunta amb una o més parts, que se signaran en entorns controlats per l'Ajuntament. En el cas que aquest tipus de documents electrònics se signin en entorns fora del control de l'Ajuntament caldrà atenir-se al que es determina a l'apartat 9 de la present Política. Addicionalment, quan el signatari representi a una altra persona es disposarà d'evidència suficient de la seva capacitat de representació.

Les seves principals característiques són:

- La signatura electrònica es realitza sobre un document original en suport electrònic.
- El document original i les signatures s'han d'incorporar al sistema de signatura.
- La signatura electrònica haurà de ser validada mitjançant un servei o autoritat de validació amb la finalitat d'assegurar la seva integritat i autenticitat.
- El document electrònic haurà d'estar en qualsevol dels formats admesos per l'Ajuntament, preferiblement en PDF/A i XML, amb l'objectiu de garantir la seva preservació al llarg del temps.
- El document electrònic es podrà signar més d'una vegada, per part de diverses persones usuàries i de forma paral·lela o seqüencial.

En relació amb els tipus de signatura aplicables a aquest cas, s'estableixen els següents requeriments:

Classes de signatura	• Signatura múltiple qualificada o avançada per part de l'Ajuntament, en combinació amb qualificada, avançada, l'ús de claus concertades o l'ús de claus concertades amb complement de doble factor d'autenticació i, en el cas de tercers, biometria d'acord amb el descrit als apartats 7.1.a, 7.1.b, 7.1.d, 7.1.e i 7.1.f.
Tipus de certificat	• Per les signatures generades per part de l'Ajuntament: Certificat de representant o d'empleat públic. • Per les signatures generades por tercers, qualsevol certificat de signatura que acrediti la voluntat d'una persona física o jurídica dels contemplats a l'apartat 6.2.
Formats acceptats	• "PAdES-LTV" amb segell de temps o "XAdES-B-T" (d'acord amb el que determini la Política de signatura i certificats de l'AGE vigent).
Nivell de signatura	• Múltiple (seqüencial o paral·lela)
Aplicació de segell de temps	

8.5 Signatura electrònica automatitzada

Aquest cas d'ús permet la signatura de documents electrònics de forma automàtica amb plenes garanties jurídiques mitjançant l'ús de certificats de segell electrònic sense la intervenció de persones signants en el procés.

Aquest supòsit està pensat per a aquelles tasques en les quals s'han de signar documents de forma automatitzada amb plenes garanties jurídiques. Per a la seva execució es farà servir un certificat electrònic que signarà els documents en nom de l'aplicació en qüestió i de l'Ajuntament.

Les seves principals característiques són:

- La signatura electrònica es realitza sobre un document original en suport electrònic de forma automàtica.

- El document electrònic podrà estar en qualsevol dels formats admesos per l'Ajuntament (PDF, PDF/A i XML), encara que es preferirà l'ús del format PDF/A per a documents que s'hagin de remetre a les persones interessades.

- Els certificats digitals i les claus privades que permeten generar processos de signatura automatitzada es guardaran en un repositori segur en els servidors de l'Ajuntament o en un servidor d'una tercera entitat prestadora de serveis, sempre que aquesta cessió estigui limitada i controlada d'acord amb el que disposa l'apartat 6.5.2.

En relació amb els tipus de signatura aplicables en aquest cas, s'estableixen els següents requeriments:

Classes de signatura	• Avançada, d'acord amb el que descriu l'apartat 7.2.a. • CSV, d'acord amb el que descriu l'apartat 7.2.b.
Tipus de certificat	• Certificat de segell electrònic • Per a les signatures generades per tercers, qualsevol certificat de signatura contemplat a l'apartat 6.
Formats acceptats	• Per documents PDF o PDF/A: "PAdES-LTV" amb segell de temps. (d'acord amb el que determini la Política de signatura i certificats de l'AGE vigent).
Nivell de signatura	• Simple
Aplicació de segell de temps	

8.6 Signatura electrònica per a digitalització segura

Aquest cas d'ús consisteix en la signatura electrònica d'un document digitalitzat en format PDF o PDF/A, amb la finalitat de crear una còpia autèntica electrònica. La seva signatura és clau per a garantir la integritat i autenticitat del document digitalitzat.

Signaran electrònicament el document:

- L'empleat públic habilitat que digitalitzi el document, en el cas que es procedeixi al control manual i acarament de l'original.
- Un segell electrònic del sistema de l'Ajuntament en el cas d'actuació administrativa automatitzada.

En relació amb els tipus de signatura aplicables en aquest cas, s'estableixen els següents requeriments:

Classes de signatura	• Avançada, d'acord amb el que es descriu en els apartats 7.1.a i 7.2.a. • CSV, d'acord amb el que descriu l'apartat 7.2.b.
Tipus de certificat	• Certificat d'empleat públic. • Certificat de segell electrònic.
Formats acceptats	• *"PAdES-LTV"*. (d'acord amb el que determini la Política de signatura i certificats de l'AGE vigent).
Nivell de signatura	• Simple.
Aplicació de segell de temps	

8.7 Signatura de persones no nacionals ni residents

L'Ajuntament de Tarragona admet tots els certificats digitals reconeguts per les autoritats homologades pel Ministeri corresponent del Govern estatal d'acord amb el Reglament eIDAS. Aquesta admissió pot quedar limitada per les capacitats de les eines d'interpretació i validació de certificats que usi l'Ajuntament.

S'estableixen les següents directrius amb relació a la identificació i signatura de persones no nacionals ni residents en l'àmbit de l'Ajuntament:

- Preferentment, les persones físiques i jurídiques, en la seva relació amb l'Ajuntament, hauran d'obtenir un certificat digital dels descrits a l'apartat 6.2, que es podrà obtenir per part d'una entitat de certificació del seu país. En el cas de ciutadans residents a la UE, el reconeixement serà automàtic d'acord amb els prestadors de serveis de confiança electrònica qualificats reconeguts pel Reglament eIDAS, mentre que, en el cas d'emissors de certificats situats fora de la UE, caldrà verificar la solvència de l'Autoritat de Certificació emissora del certificat corresponent.

- En defecte de l'anterior, es podran fer ús de la resta dels mitjans de signatura electrònica identificats a l'apartat 7.1 i que puguin ser usats per terceres parts, concretament, els sistemes de signatura contemplats en els apartats 7.1.a, 7.1.b, 7.1.d i 7.1.e.

8.8 Incorporació de documents electrònics signats de fonts externes

Pel que fa a les signatures provinents de plataformes alienes a l'Ajuntament, es procedirà a la seva validació, i, un cop validades, s'incorporaran a l'expedient amb les corresponents evidències de validació.

En aquest sentit, el següent apartat 9 preveu les comprovacions a realitzar per procedir a la validació de signatures de tercers.

9. Comprovacions a tenir en compte en la validació de signatures electròniques de tercers realitzades amb certificat digital

L'Ajuntament de Tarragona implementarà controls automàtics per a validar les signatures electròniques. Quan no sigui possible fer-ho així, es capacitarà el personal de l'Ajuntament perquè també pugui realitzar-los de forma manual, fent ús dels sistemes de validació que s'identifiquen en els apartats 9.1 i 9.2 de la present Política.

Així doncs, per a garantir la validesa jurídica dels documents electrònics signats digitalment, qualsevol document que entri a l'Ajuntament que contingui una signatura o un segell de temps, prèviament al seu emmagatzematge en el gestor documental, ha de ser validat.

Per a fer-ho, pot emprar algun d'aquests sistemes automàtics:

- **Signasuite**, el servei online del Consorci AOC que permet determinar la validesa de signatures i certificats digitals.

- **VALIDe,** el servei online de l'Administració General de l'Estat (AGE) que permet determinar la validesa de signatures i certificats digitals.

- **Adobe Acrobat Reader,** software a través del qual els documents signats en format *"PAdES"* també poden avaluar la validesa d'una signatura digital comprovant les seves propietats. Quan s'obté el document en format *".pdf"* signat, és possible validar la seva signatura per verificar el signant i el contingut signat. En funció de com s'hagi configurat l'aplicació, la validació es pot efectuar de forma automàtica. En aquest sentit, la validesa de la signatura està determinada per la verificació de l'autenticitat de l'estat del certificat digital i la integritat del document signat. La verificació de l'autenticitat confirma que el certificat de la persona signant o els seus certificats principals existeixen en la llista d'identitats de confiança del validador. Per altra banda, també confirma si el certificat de signatura és vàlid segons la configuració que hagi determinat la persona usuària. La verificació d'integritat del document confirma si el contingut signat ha canviat després de la seva signatura; si canvia, la verificació d'integritat del document confirma si el contingut ha variat d'una manera permesa pel signant.

- Altres sistemes que l'Ajuntament pugui desenvolupar en un futur.

Pel que fa a les signatures electròniques realitzades mitjançant certificat, només en aquells casos en què el procés de validació de totes les signatures electròniques i dels segells electrònics sigui satisfactori, es pot procedir a emmagatzemar el document electrònic dins del gestor documental de l'Ajuntament.

En relació a les signatures electròniques efectuades a través de l'acreditació de la identitat i la captura d'evidències de la voluntat de signatura o de dades biomètriques, s'ha d'emmagatzemar el document electrònic amb les seves signatures en el gestor documental directament, sense cap validació addicional, ja que els sistemes de signatura d'aquest tipus són suficientment segurs i no compten amb un procés de validació automàtica. En aquests casos es procedirà a la signatura electrònica del document amb un certificat de segell electrònic en format -T. Així doncs, només procedeix completar la signatura amb aquesta signatura secundària, havent només de comprovar la seva validesa de la mateixa forma indicada per a la validació de les signatures realitzades amb certificat digital.

9.1 Comprovacions manuals de la validesa de la signatura electrònica

En el cas en que les comprovacions automàtiques de les signatures electròniques resultin incorrectes, caldrà procedir a la seva verificació manual, tal i com s'exposa en els següents apartats.

9.1.1 Verificació de la data de signatura

La data de signatura d'un document electrònic és rellevant per gestionar la validesa del certificat de la persona signant. És possible que el document electrònic tingui una data de signatura en el seu contingut, però que aquesta no coincideixi amb la data de la signatura electrònica. En conseqüència, cal verificar la data en què s'ha signat el document i diferenciar si la data de signatura s'ha establert mitjançant un segell de temps o usant el rellotge del dispositiu de la persona signant. Només en el cas que la data de la signatura electrònica provingui d'un segell de temps, existirà una seguretat fidedigna del moment en què es va produir la signatura, amb independència de la data que consti en el contingut del document electrònic. Si bé aquestes comprovacions es realitzaran de forma automàtica mitjançant l'aplicació de captura del document, també es podran efectuar manualment per part del personal de l'Ajuntament.

9.1.2 Identificació de la titularitat i la cadena de confiança

La generació d'una signatura electrònica requereix l'ús d'un certificat digital reconegut, que haurà de ser necessàriament emès per part d'una entitat prestadora de serveis electrònics de confiança qualificats. Aquest fet permet acreditar que la signatura electrònica usada és segura i garantir la identitat de la persona signant.

Si la verificació de l'emissor del certificat digital falla, sigui automàticament o manualment, l'Ajuntament no dipositarà la seva confiança en la signatura del document electrònic i aquest serà rebutjat i retornat a la persona signant, indicant que no podrà ser admès a causa que la signatura electrònica no ha estat realitzada amb un certificat digital emès per un prestador de serveis electrònics de confiança qualificat.

9.1.3 Verificació de la vigència del certificat

Els certificats digitals podran caducar d'acord amb la data fixada en el moment de la seva emissió, o fins i tot ser suspesos o revocats abans d'aquesta data per diversos motius, com, per exemple, la pèrdua de vigència de les dades dels certificats o la pèrdua de la targeta criptogràfica.

Tenint en compte l'exposat en el paràgraf anterior, l'Ajuntament haurà de comprovar la validesa de les signatures emeses d'acord amb les dades aportades pel certificat o l'autoritat de certificació seguint els següents procediments:

- Verificació de les llistes de revocació de certificats "CRLs", implementades automàticament per la majoria de les aplicacions que permeten la visualització dels documents signats del mercat, malgrat que no generin proves concretes.

- Sol·licitud d'un informe de verificació per part del prestador de serveis de certificació, però que s'haurà de sol·licitar mitjançant un sistema informàtic de l'Ajuntament.

És possible que el certificat caduqui després de la signatura d'un document electrònic. Per aquest motiu, és important que l'Ajuntament sigui capaç d'acreditar que el certificat era vigent en la data d'emissió de la signatura mitjançant l'aplicació d'un segell de temps emès per una autoritat de segellament de temps (TSA), segons l'exposat a l'apartat 7.2.c.

9.1.4 Verificació de la vinculació criptogràfica del document amb la signatura

Aquesta verificació es duu a terme per validar que la signatura electrònica fa referència al document que s'al·lega haver signat, ja que és possible que el document pugui haver sofert modificacions posteriors al moment de la seva signatura, per la qual cosa la signatura ja no es correspondrà amb el contingut del document, evidenciant un problema d'integritat del mateix.

En els processos d'incorporació del document en el sistema de gestió documental de l'Ajuntament, la verificació es durà a terme mitjançant un procediment de validació automàtica. No obstant això, aquesta comprovació també es podrà efectuar manualment mitjançant l'ús d'aplicacions ofimàtiques que permetin la visualització de documents signats electrònicament i la interpretació de la validesa de la seva signatura.

Quan aquest procés de verificació falli, es considerarà que la signatura és defectuosa i es procedirà a la devolució del document electrònic al seu emissor, informant del motiu de rebuig.

9.2 Comprovacions manuals de la validesa de la signatura electrònica en relació amb el signant i el seu contingut

En qualsevol cas, després de les comprovacions automàtiques i manuals anteriors s'hauran de realitzar una sèrie de comprovacions manuals relacionades amb la capacitat de signatura per part del signant i el contingut del document que es detallen a continuació.

9.2.1 Identitat de la persona titular del certificat

Tenint en compte que un certificat digital proporciona informació per identificar la persona física o jurídica que es compromet amb el contingut del document, verificar la seva identitat mitjançant les referències que es puguin extreure del certificat digital resulta clau per poder establir que un document ha estat signat per la persona que al·lega haver-ho fet. En el cas de signatura mitjançant representació, hi haurà de constar informació del representant i de la persona representada en el camp corresponent. Si el titular del certificat coincideix amb la persona que consta com a signant del document o el seu representant, es pot donar la verificació per vàlida, mentre que en el cas que el titular del certificat no coincideixi amb la identitat de la persona que hauria de signar el document, s'haurà de rebutjar el document per no poder-se admetre la seva signatura.

9.2.2 Validació de les facultats de la persona signant

És possible que algunes vegades se signi en nom d'un tercer. En aquest cas, l'Ajuntament haurà de comprovar que la persona signant està capacitada per a exercir la representació al·legada, en el cas que aquestes facultats no constin en el propi certificat digital o no es puguin comprovar com, per exemple, el nivell de capacitat de representació segons l'import d'una transacció econòmica. És per això que, en alguns casos, pot resultar adequat requerir la presentació de documentació addicional que permeti acreditar la representació o optar per la opció de verificar la seva identitat mitjançant l'accés a registres externs. Quan no sigui possible verificar la suficiència de poders de representació de la persona signant, s'haurà de retornar el document al seu emissor.

9.2.3 Verificació del contingut del document proposat per l'Ajuntament per a la signatura d'un tercer

La verificació del contingut d'un document electrònic resulta tan crucial com la d'un document en paper. Tot i que en el cas del document electrònic, les comprovacions es centren en l'anàlisi sobre l'adequació del contingut i si s'ajusta als requisits necessaris per gaudir de validesa jurídica. En el cas que el document s'hagi produït en origen pel mateix Ajuntament, es recomana fer-lo signar al tercer, prèvia signatura mitjançant un segell electrònic del propi Ajuntament, per tal d'automatitzar la verificació del retorn mitjançant la comprovació de la signatura electrònica de segell electrònic, tal com s'ha exposat a l'apartat 9.1.4. Si no es pot verificar de forma automàtica, s'haurà de revisar manualment el contingut del document per garantir que no s'ha produït cap canvi entre la versió remesa a la persona signant i la versió que es retorna signada. Si la verificació falla, es procedirà a la devolució del document signat pel tercer i/o a requerir la documentació addicional que pugui acreditar la capacitat de representació.

10. Estratègia de preservació de documents i signatures electròniques

Malgrat que la signatura electrònica permet acreditar l'autenticitat de l'expressió de la voluntat en documents electrònics, hi ha certs riscos que s'han de gestionar degudament per garantir la validesa jurídica indefinida del document electrònic.

Aquests riscos són:

- La caducitat o revocació del certificat digital o del segell electrònic mitjançant el qual se signa un document electrònic.
- L'absència de validesa del certificat digital o del segell electrònic en el moment en què es genera la signatura electrònica.
- La possible obsolescència tecnològica de la longitud de les claus criptogràfiques contingudes en els certificats digitals mitjançant els quals es generen signatures electròniques.

Per a garantir la validesa de les signatures electròniques rebudes i emeses per l'Ajuntament, l'estratègia adoptada es basa en un model d'evidències d'integritat que ofereix el sistema de gestió de documents electrònics quan emmagatzema els documents un cop signats correctament. Per aquest motiu, totes les signatures electròniques de documents rebuts s'han de validar abans de la seva incorporació en el sistema de gestió de documents electrònics i rebutjar-se en cas que no siguin vàlides.

Per garantir el manteniment i la preservació de les signatures electròniques, i contrarestar així els riscos ja esmentats, l'Ajuntament es dota dels mecanismes de preservació de documents i signatures mitjançant ressegellat de temps i mitjançant evidències segures del sistema de gestió documental, que es podran emprar indistintament o de manera complementària.

Així doncs, a continuació es descriu com aplicar aquests mecanismes en funció de l'entorn:

10.1 Ressegellat i preservació de documents i signatures electròniques en entorns propis

El procés de ressegellat consisteix en la renovació del segell de temps aplicat al document electrònic, mitjançant la incorporació d'un nou esglaó en la cadena d'evidències electròniques a les signatures electròniques que el document ja conté. L'objectiu principal del procés és garantir la conservació, integritat i autenticitat del document electrònic al llarg del temps.

El ressegellat s'aplicarà a aquells documents electrònics que no hagin estat transferits a la solució d'arxiu electrònic únic de l'Ajuntament en el moment en què estigui a punt de caducar l'últim segell de temps aplicat a la signatura electrònica a preservar i, de forma excepcional, quan s'hagi detectat l'obsolescència tecnològica dels algorismes o claus que signen el document en qüestió.

Aquest procés requereix que les signatures del document estiguin en format "XAdES-A" o "PAdES-LTV", que són els tipus de signatura que admeten l'afegiment d'evidències temporals. En el cas que la signatura no estigui en un dels dos formats, abans de dur a terme el procés de ressegellat, caldrà completar la signatura dels documents en un dels formats indicats.

S'afegirà llavors un nou segell de temps a les signatures "XAdES-A" o "PAdES-LTV" que haurà de:

- Estar generat amb un certificat recent.
- Tenir període de validesa superior a les signatures que cal ressegellar.
- Tenir una longitud de clau suficient amb l'objectiu que no pugui resultar compromesa.
- Aplicar un algorisme o clau que no estigui subjecte a l'obsolescència criptogràfica del mateix en el moment en què s'emet.

Pel que fa a les signatures realitzades mitjançant l'acreditació de la identitat i la recollida d'evidències de la voluntat de signatura, es procedirà al ressegellat de la signatura secundària, és a dir, el segell de temps que garanteix la integritat del document.

Quan l'Ajuntament pretengui revisar la validesa de les signatures electròniques, durà a terme els següents passos per a cada tipus de signatura:

- En el cas de signatures electròniques generades dins els entorns sota el control de l'Ajuntament es procedirà a la generació de les signatures en formats que permetin garantir la seva preservació durant la fase de tramitació del procediment administratiu. En conseqüència, per als documents en format XML, les signatures es transformaran al format *"XAdES-A"* i per als documents PDF, en format *"PAdES-LTV".*
- Quan les signatures electròniques provinguin de plataformes externes es procedirà a completar-les en un moment posterior al tancament i foliació de l'expedient administratiu. En conseqüència, per als documents en format XML, les signatures es transformaran al format *"XAdES-A"* i per als documents PDF, en format *"PAdES-LTV"*.
- Quan per qualsevol motiu no sigui possible generar signatures electròniques amb garanties de preservació, es procedirà, el més breument possible, a generar una còpia electrònica autèntica del document original. Aquest procés resultarà en l'aplicació d'una signatura en

format que garanteixi la preservació de la còpia electrònica autèntica, que substituirà el document original.

- Pel que fa a les signatures electròniques basades en la identitat més la voluntat de signatura, es generarà la signatura mitjançant l'aplicació del segell electrònic en un format que garanteixi la preservació, preferentment *"PAdES-LTV"*.
- En el cas de les signatures electròniques basades en CSV, es mantindrà una versió del document electrònic guardada en els repositoris de consulta, amb les signatures electròniques en formats que garanteixin la seva preservació.
- En referència a les firmes biomètriques, es generarà signatura electrònica mitjançant l'aplicació d'un segell electrònic en format que garanteixi la seva preservació (*"PAdES-LTV"*).

10.2 Preservació de documents i signatures electròniques mitjançant evidències segures del sistema de gestió documental

Aquest mecanisme de preservació de documents i signatures electròniques suposa l'ús d'evidències segures del sistema de gestió de documents electrònics de l'Ajuntament. Aquest mètode implica, en primera instància, la confiança en el sistema de gestió documental emprat per l'Ajuntament, ja que és el propi sistema el que garanteix la integritat dels documents incorporats en el sistema. D'aquesta manera, aquells documents que no presentin una signatura electrònica vàlida no seran incorporats en el gestor documental o si ho són quedarà constància de que no eren vàlids en el moment de la seva incorporació.

En aplicació d'aquesta estratègia de preservació, sempre que s'emmagatzemi un document, es generarà i guardarà el "hash" o resum criptogràfic associat al mateix en forma de metadada de gestió documental i com a mesura per garantir la seva integritat. Així mateix, i amb la finalitat de garantir la validesa del "hash", l'Ajuntament aplicarà les mesures de vigilància necessàries en el sistema que s'utilitzi, segons les solucions tecnològiques disponibles en cada moment, garantint en tot moment la integritat i inviolabilitat de la informació sobre el "hash" i la seva vinculació amb el document corresponent.

Així mateix, es procedirà a una actualització del mètode de càlcul del "hash" en cas que l'anterior pugui veure's compromès, generant un nou "hash" i guardant alhora el "hash" anterior com a mesura addicional que permeti garantir la integritat del document. En consultar un document emmagatzemat en el sistema de gestió de documents electrònics de l'Ajuntament, s'hauran de comprovar les evidències d'integritat mitjançant l'acarament del "hash" obtingut i l'emmagatzemat en el sistema de gestió documental per a aquest document. En el cas que coincideixin, es podrà obtenir una còpia autèntica per a la seva consulta generada mitjançant actuació administrativa automatitzada i signada electrònicament amb CSV, d'acord amb

l'exposat a l'apartat 7.2.b de la present Política i/o signatura amb segell electrònic d'actuació administrativa automatitzada segons l'exposat a l'apartat 7.2.a

La còpia autèntica generada no serà emmagatzemada en atenció a que pot tornar a ser generada en qualsevol moment, ja sigui perquè existeixi una nova consulta o perquè s'introdueixi un CSV per a la seva comprovació. Per tant, el CSV quedarà vinculat al document de forma inequívoca, de manera que per a cada nova consulta es generi amb el mateix CSV o es pugui comprovar la seva integritat a partir del propi CSV.

Quan s'empri aquest sistema de preservació no serà necessari el ressegellat de les signatures electròniques, ja que és el sistema el que aporta les garanties i la certesa que les signatures no han estat modificades o alterades des del seu emmagatzematge, gràcies a les mesures de seguretat que apliqui l'Ajuntament.

10.3 Preservació de documents i signatures electròniques mitjançant evidències segures del sistema de gestió documental. Preservació de documents i firmes electròniques en expedients transferits a l'arxiu electrònic únic

10.3.1 Selecció de formats documentals de conservació

Les actuacions que permeten la preservació del format del document, els seus elements de seguretat, signatures electròniques i segells de temps són necessàries per garantir la intel·ligibilitat i integritat dels documents electrònics a llarg termini.

D'acord amb el paràgraf anterior, el sistema de preservació de documents electrònics ha de realitzar controls periòdics sobre aquests mateixos per garantir la seva accessibilitat, la possibilitat de recuperar-los i la seva validesa jurídica, que comprovaran:

- L'accessibilitat dels seus suports.
- La capacitat de lectura dels seus formats.
- La validesa jurídica de les signatures electròniques.
- La integritat dels documents.
- La integritat dels expedients.

En el cas que els documents provinguin d'una font externa a l'Ajuntament, es proposa la seva conversió al format PDF/A, que, en el moment d'elaboració de la present Política, és el format més usat per a la preservació de documents electrònics. El format PDF també s'acceptarà sempre que provingui d'aplicacions corporatives existents que generin documents en tal format.

Amb la finalitat de garantir la validesa de la signatura electrònica, s'aplicarà el criteri establert prèviament que consisteix a completar les signatures existents en formats que permetin garantir la seva preservació al llarg del temps, concretant-se aquests en:

- "XAdES-A" per als documents en format XML amb signatures "XAdES".
- "PAdES-LTV" per als documents en format PDF o PDF/A.

Partint d'aquestes signatures, i en el moment en què el segell electrònic caduqui, es procedirà al ressegellat de les signatures electròniques mitjançant l'aplicació d'un nou segell, amb una caducitat suficient i amb els algorismes o claus de signatura actualitzats.

El format aplicat al foliat de l'expedient serà XML, atès que és el format que permet una millor actuació administrativa automatitzada garantint la integritat de l'expedient.

10.3.2 Requeriments dels elements a transferir a l'eina d'arxiu

Els elements seleccionats per a la seva transferència a l'eina d'arxiu electrònic únic hauran de complir amb els requeriments següents:

- Els expedients hauran d'estar en l'eina de gestió documental, tancats i foliats de forma íntegra amb els documents que en formen part i amb els resums criptogràfics d'aquests.
- Les metadades obligatòries dels documents, expedients i signatures hauran d'estar informats de forma correcta.
- Els documents electrònics hauran d'estar en un format reconegut, gestionable i no obsolet segons l'eina d'arxiu electrònic únic utilitzada.
- Les signatures electròniques dels documents i expedients hauran d'estar completades en formats que en garanteixin la preservació.

10.3.3 Manteniment i migració de formats

Malgrat que en origen es determinin els formats que puguin garantir una major preservació dels documents al llarg del temps, cal tenir en compte la possibilitat que aquests formats puguin acabar quedant obsolets, sigui per motius de seguretat o per la seva substitució per altres tecnologies que provoquen que els formats deixin de ser estàndards comunament acceptats.

Els documents en format obsolet o en procés d'obsolescència s'hauran de migrar a nous formats més adequats que permetin complir amb les funcions de preservació.

L'Ajuntament considera que la migració és l'opció més recomanable per poder garantir l'accés a la documentació amb independència del temps transcorregut, mitjançant l'aplicació de les

recomanacions dels estàndards internacionals ISO 18493:2018 i el model OAIS (Sistema d'informació d'arxiu obert) definit a l'estàndard ISO 14721:2003.

La implementació tecnològica de la migració dependrà de les solucions tecnològiques disponibles en cada moment. De totes maneres, es contemplen dues alternatives:

- Definir un procediment de migració certificat dins del propi sistema de gestió de documents electrònics o de l'arxiu electrònic únic de l'Ajuntament, sempre que el procediment sigui capaç de garantir l'equivalència funcional entre el document original i el resultant del procés i certificar la migració mitjançant l'aplicació de les mesures d'autenticitat corresponents.
- Delegar el procés de migració a un tercer de confiança mitjançant l'ús d'una plataforma que permeti transferir i recuperar els documents de forma segura, sempre que el document resultant compleixi amb els elements del paràgraf anterior.

Sempre que el document resultant contingui signatures electròniques criptogràfiques vinculades al resum criptogràfic del document original, la signatura i document original es conservaran amb la finalitat de poder seguir acreditant la seva autoria, malgrat que la consulta i intel·ligibilitat del document estaran garantides en el document resultant de la migració.

11. Manteniment de la Política

11.1 Desplegament de la Política d'identitat i signatura electròniques

L'actualització de la present Política requerirà que es dugui a terme l'adequació de les diverses aplicacions, eines informàtiques i processos que s'utilitzin a l'Ajuntament. En aquest cas, el Servei de Tecnologies de la Informació i les Comunicacions coordinarà l'actualització de tots els sistemes afectats per adequar-los al que disposa la present Política en un termini d'un any des de la seva aprovació.

Els serveis i sistemes que es posin en funcionament amb posterioritat a l'entrada en vigor de la present Política d'identitat i signatura electròniques de l'Ajuntament estaran subjectes a aquesta des del moment en què comencin a operar.

El Servei de Tecnologies de la Informació i les Comunicacions haurà d'examinar, amb una periodicitat bianual, amb la finalitat de comprovar l'estat de compliment de la Política, la seva adequació a les necessitats reals de l'Ajuntament i el seu alineament amb les tecnologies disponibles, informant-ne a Secretaria.

11.2 Situacions transitòries

Els mètodes d'identificació i signatura contemplats en la present Política es començaran a utilitzar de forma progressiva, conforme l'Ajuntament disposi de les aplicacions, eines i processos necessaris per al seu ús.

S'actualitzaran els sistemes afectats en el termini de sis mesos a partir de l'aprovació d'aquesta Política amb la finalitat d'adequar-los a les seves disposicions.

11.3 Derogació d'estàndards obsolets

L'aprovació de la present Política d'identitat i signatura electròniques suposa la derogació dels estàndards tècnics d'identificació i signatura i altres documents de desenvolupament que la contradiguin.

11.4 Entrada en vigor

La present Política entrarà en vigor en el moment de la seva publicació a la seu electrònica, on hi haurà disponible el text íntegre del document per a la seva consulta.

Annex I – Glossari i conceptes de signatura electrònica

Glossari

S'ha considerat adient la incorporació d'un annex de definició de conceptes aplicats en aquest document, amb la finalitat de fer-lo més comprensible.

- **Casos d'ús de la signatura electrònica:** Fa referència als casos d'ús de la signatura electrònica, entesos com els possibles escenaris de generació de documents electrònics signats. Per cada cas d'ús s'identifiquen els formats de signatura electrònica aplicables, els possibles nivells de signatura, etc.

- **Classes de signatura electrònica:** Aquest document es refereix a les classes de signatura electrònica i a la seva validesa jurídica, que, segons es defineix en el Reglament eIDAS, es classifiquen en signatura simple, avançada i qualificada.

- **Format de signatura electrònica:** La forma en què es codifiquen les firmes electròniques, sent els seus formats més comuns: *"S / MIME"*, *"CMS", "XAdES", "CAdES"* i *"PAdES".*

- **Nivell de signatura:** Fa referència a si el document disposa d'una o múltiples signatures i si en aquest cas es generen de forma paral·lela o seqüencial.

- **Segellament de temps:** Consisteix en una acreditació de la data i hora de realització de qualsevol operació o transacció per mitjans electrònics a càrrec d'un tercer de confiança.

- **Sistema de signatura:** Es refereix a la forma de signatura d'un document electrònic, sigui mitjançant un certificat digital de la persona signant, per mitjà d'un sistema d'identificació més evidència electrònica de l'acte de signatura, signatura biomètrica o mitjançant un CSV.

- **Tipus de signatura:** Indica la forma de relació de la signatura electrònica amb el document signat, dins del mateix document, com un document a part, dins d'estructures XML, etc.

Els actors involucrats en el procés de creació i validació d'una signatura electrònica són els següents:

- **Signant:** Persona que posseeix un dispositiu de creació de signatura i que actua en nom propi o en nom d'una persona física o jurídica.

- **Creador d'un segell:** Persona jurídica que crea un segell electrònic.

- **Verificador:** Entitat, sigui persona física o jurídica, que valida o verifica una signatura electrònica recolzant-se en les condicions exigides per la política per la qual es regeix la plataforma de

relació electrònica, o el servei concret en el qual s'està invocant. Podrà ser una entitat de validació de confiança o una tercera part que estigui interessada en la validesa d'una signatura electrònica.

- **Prestador de serveis de signatura electrònica:** Una persona física o jurídica, que expedeix certificats electrònics o presta altres serveis relacionats amb la signatura electrònica.

Aquest document fa servir el concepte "signant" per referir-se tant a la persona que signa com al creador d'un segell. En aquest darrer cas, es pot tractar d'un procés d'actuació administrativa automatitzada.

Conceptes de signatura electrònica

Definició jurídica de la signatura electrònica

Des d'una perspectiva jurídica, les diferents classes de signatura es defineixen com:

- **Signatura electrònica Simple:** Conjunt de dades en forma electrònica, consignades juntament amb altres o que estan associades, que poden ser usades com a mitjà d'identificació de la persona signant. Entenent la identificació com a autenticació davant les entitats.

- **Signatura electrònica Avançada:** Conjunt de dades en forma electrònica que permeten identificar el signant i detectar qualsevol canvi posterior de les dades que s'hagin signat, vinculada al signant de forma única i a les dades a què fa referència, creada per mitjans que el signant pot mantenir sota el seu control exclusiu.

- **Signatura electrònica Qualificada:** Signatura electrònica avançada basada en un certificat reconegut i que ha estat generada mitjançant un dispositiu segur de creació de signatura.

El concepte de certificat reconegut a què es refereix a les definicions del present apartat es refereix a aquells certificats electrònics emesos per un prestador de serveis de certificació, que compleixen amb els requisits establerts pel que fa a la comprovació de la identitat i la resta de les circumstàncies dels sol·licitants i a la fiabilitat i garanties dels serveis de certificació que presten.

Fonaments tècnics de la signatura electrònica

Des d'un punt de vista tècnic, els **tipus de signatura** es defineixen com:

- **Signatura "*attached*":** Les dades de la signatura electrònica resideixen en el document signat. Per tant, el mateix document disposa de tota la informació necessària per comprovar

l'autenticitat i integritat d'aquest, així com la informació necessària per validar la signatura. Existeixen dos tipus diferents de signatura "*attached*":

- **"*Enveloped*" (incrustada):** El document electrònic disposa del contingut i de la seva signatura.
- ***"Enveloping" (imbricada):*** *El fitxer de signatura serveix de signatura del document electrònic a signar, el qual s'inclou dins del propi fitxer de signatura.*

- **Signatura "detached":** Les dades de la signatura electrònica resideixen fora del document a signar, però associades a aquest. Les dades de la signatura es mantindran per separat durant tot el cicle de vida del document. Per validar la signatura cal crear un document d'evidències electròniques que contingui conjuntament el document i les dades completes de la signatura.

En relació amb el nivell de signatura:

- **Signatura simple:** El document conté una única signatura.
- **Signatura múltiple:** El document conté dues o més signatures. La signatura múltiple consisteix que diversos signants signin el document de forma consecutiva. Aquest tipus de signatura es pot aplicar sobre el document original cada vegada (signatura paral·lela) o sobre el document signat (signatura seqüencial).

La signatura múltiple es farà servir en diverses actuacions en el marc dels procediments de l'Ajuntament, com, per exemple, en la signatura de documents electrònics per més d'una persona o el ressegellat de documents ja signats per actualitzar la seva validesa legal al llarg del temps, abans que la validesa criptogràfica de la signatura electrònica pugui quedar en entredit.