Agtic

Política d'Identificació i Signatura Electrònica

AJUNTAMENT DE MONT-ROIG DEL CAMP

Amb el suport del Departament de Cultura

Generalitat de Catalunya
Departament de Cultura

Desembre de 2022

CONTINGUT

1. Introducció

L'Ajuntament de Mont-roig del Camp, en la seva estratègia d'implantació del document i l'expedient electrònic com a element de base per evidenciar la seva actuació administrativa, d'acord amb la Llei 39/2015 de Procediment Administratiu Comú de les Administracions Públiques, requereix dotar-se d'una Política d'Identificació i Signatura Electrònica, tal i com estableix la 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 Política de Signatura Electrònica i segells electrònics i de certificats de l'Administració.

Aquesta Política ha de garantir l'ús correcte de les eines de signatura electrònica amb l'objectiu que es permetin generar amb caràcter d'autenticitat documents electrònics, expedients electrònics i foliats d'expedients electrònics. Per aquest motiu, la present Política es fonamenta en els següents criteris:

- La voluntat de l'Ajuntament que la seva activitat administrativa es plasmi en documents i expedients electrònics autèntics.
- Els documents electrònics originals signats electrònicament, en compliment del que estableix aquesta Política, tindran plena validesa i es presumiran autèntics.
- El nivell de seguretat tecnològica, el tipus de certificat a utilitzar, el format de la signatura i del segellat de temps i els mecanismes de preservació es fixaran en funció de la importància del document, de l'acte administratiu al qual facin referència i de la taula d'accés i avaluació documental aplicable.
- Les signatures electròniques que es generen a l'Ajuntament es faran amb el format i el nivell de seguretat requerits per a la seva conservació durant tot el període de vida útil del document al qual referencien.
- Els documents electrònics que es rebin signats seran sotmesos a un procés de validació i completesa de les signatures en el moment de la recepció.

En aquest sentit, en aquesta Política es desenvolupen els següents elements:

1. L'objecte amb el qual es desenvolupa la Política d'Identificació i Signatura Electrònica de l'Ajuntament de Mont-roig del Camp.
2. Les dades identificatives de la Política, els seus períodes de validesa i la seva transició a noves polítiques i l'assignació de responsabilitats per a la seva gestió i aplicació.
3. La definició dels conceptes clau en matèria de signatura electrònica i que són desenvolupats al llarg de la Política.
4. La normativa i els estàndards internacionals als que es troba subjecta la Política i en base als quals es desenvolupa.

5. L'ús de certificats digitals i altres identitats digitals:
    - *Certificats digitals i identitats digitals admeses:* quins certificats digitals o identitats digitals (acreditades a través d'un registre previ) poden utilitzar altres persones o entitats per relacionar-se telemàticament amb l'Ajuntament i com s'actualitzarà i publicarà la llista de certificats admesos.
    - *Certificats digitals emprats:* quins certificats digitals poden utilitzar els treballadors de l'Ajuntament en l'exercici de les seves funcions i els segells electrònics que estan previstos per a l'actuació automatitzada.
    - *Signatura electrònica basada en identitats digitals i evidències electròniques associades a la voluntat de la signatura*, tal i com es recull al Capítol segon del Títol I de la Llei 39/2015, de Procediment Administratiu Comú de les Administracions Públiques.
6. El cicle de vida dels certificats emprats per l'Ajuntament, identificant-se com es poden obtenir els certificats quan es necessitin i com es portarà el control dels certificats existents i de la seva eventual revocació quan deixin de ser necessaris.
7. La definició del segell de temps com a element que permet deixar evidència de la data i l'hora en què s'ha produït un acte.
8. Els diferents sistemes d'identificació emprats en l'àmbit de l'Ajuntament.
9. Les classes, tipus i nivells de signatura, és a dir, el com i en quin format es generen les signatures electròniques emprades en l'àmbit de l'Ajuntament, així com el procés seguit per a la seva validació.
10. Els Codis Segurs de Verificació (CSV) com a mètode de signatura automatitzada amb segell d'òrgan en el context de l'Actuació Administrativa Automatitzada.
11. El manteniment i la preservació de signatures electròniques per garantir la introducció en els sistemes de gestió documental de l'Ajuntament de documents autèntics que garanteixin la preservació de la seva validesa jurídica a llarg termini.
12. Les normatives de signatura electrònica que tenen per finalitat determinar la validesa d'una signatura electrònica en una transacció concreta, identificant quines obligacions assumeix l'Ajuntament en cada cas, tenint en compte l'ús que s'ha de donar als documents signats electrònicament i el tipus d'actuació administrativa que recull l'acte de signatura.
13. La presentació d'un subconjunt representatiu de casos d'ús de la signatura electrònica que identifiquen possibles escenaris en els quals els procediments de l'Ajuntament poden requerir l'ús de signatures electròniques, vinculats a una normativa de signatura electrònica concreta:

- Signatura electrònica d'un document electrònic.
- Digitalització certificada de documents en paper: còpia certificada electrònica.
- Còpia electrònica certificada d'un document electrònic signat electrònicament.
- Processos de signatura automatitzada.
- Signatura electrònica biomètrica d'un document electrònic.
- Incorporació de documents signats digitalment per part d'un tercer.

Per a l'elaboració d'aquesta Política s'ha tingut en compte allò establert pel Reial Decret 4/2010 pel qual es regula l'Esquema Nacional d'Interoperabilitat, així com els següents elements de desenvolupament:

- Resolució de 27 d'octubre de 2016 (BOE de 3 de novembre), 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 la Secretaria d'Estat d'Administracions Públiques, per la qual es publica l'acord d'aprovació de la Política de Signatura Electrònica i de Certificats de l'Administració General de l'Estat i s'anuncia la publicació a la seu corresponent.
- Resolució de 19 de juliol de 2011 (BOE de 30 de juliol), de la Secretaria d'Estat per a la Funció Pública, per la qual s'aprova la Norma Tècnica d'Interoperabilitat d'Expedient Electrònic, especialment, pel que fa al seu procés de foliat.
- Resolució de 19 de juliol de 2011, de la Secretaria d'Estat per a la Funció Pública, per la que s'aprova la Norma Tècnica d'Interoperabilitat de Procediments de copiat autèntic i conversió entre documents electrònics.

2. Objecte de la Política

Aquesta Política d'Identificació i Signatura Electrònica té per objecte establir el conjunt de criteris comuns assumits per l'Ajuntament de Mont-roig del Camp en relació amb l'autenticació i el reconeixement de signatures electròniques basades tant en certificats com en evidències electròniques.

En concret, la Política estableix les directrius a seguir per l'Ajuntament de Mont-roig del Camp respecte a l'ús de la signatura electrònica, en el si de les aplicacions corporatives, per garantir l'autenticitat, la integritat i la conservació dels documents signats electrònicament. Aquesta qüestió és d'aplicació tant a les signatures com als segells electrònics.

En aquesta tessitura, la present Política també regula els nivells de seguretat, a més de les casuístiques que duen associats, dels processos d'identificació i signatura electrònics. Tanmateix, també s'estipula quins mecanismes d'identificació i signatura -per a ciutadans, empreses, treballadors públics i ens- accepta l'Ajuntament, juntament amb la classificació i descripció d'aquests segons els nivells de seguretat dels tràmits a realitzar.

Així mateix, l'objectiu d'aquesta Política és establir quines identitats digitals i quins certificats digitals de ciutadans i de tercers l'Ajuntament de Mont-roig del Camp s'accepten i quins certificats digitals utilitzen els seus treballadors establint-se també el seu cicle de vida des de que són emesos.

Finalment, aquesta Política estableix les estratègies que l'Ajuntament de Mont-roig del Camp ha d'adoptar per a la preservació a llarg termini de les signatures electròniques.

3. Dades identificatives de la Política i entrada en vigor

Les dades identificatives de la Política d'Identificació i Signatura Electrònica són els que s'inclouen a continuació:

Nom del document	Política d'Identificació i Signatura Electrònica de l'Ajuntament de Mont-roig del Camp.
Versió	0.1
Identificador de la Política	PISE.2024.01
URI de referencia de la Política	https://mont-roig.cat/lajuntament/atencio-ciutadana/arxiu-municipal/
Data d'expedició	28/11/2024
Àmbit de Aplicació	Documents i expedients produïts i/o custodiats per l'Ajuntament de Mont-roig del Camp.
Responsable de la Política	Departament de Sistemes d'Informació i Noves Tecnologies

La present Política d'Identificació i Signatura Electrònica de l'Ajuntament de Mont-roig del Camp entrarà en vigor en la data de la seva expedició i serà vàlida fins que no sigui substituïda o derogada per una altra Política posterior.

Si s'estima oportú, es podrà facilitar un període de temps transitori, en el qual convisquin dues versions de la Política, per tal de permetre adequar els diferents sistemes de signatura electrònica i validació utilitzats per l'Ajuntament de Mont-roig del Camp a les especificacions de la nova versió.

Aquest període de temps de transició s'haurà d'indicar a la nova versió i superat el mateix només serà vàlida la versió actualitzada.

4. Actors involucrats

En el context de la creació, validació i, en definitiva, gestió de les signatures i els certificats electrònics intervenen un conjunt d'actors clau per a què el procés es pugui realitzar correctament. Així doncs, els actors involucrats són els següents:

- **Signant:** Persona física que crea una signatura electrònica utilitzant dades de creació de signatura electrònica que pot utilitzar, amb un alt nivell de confiança, sota el seu control exclusiu i que actua en nom propi o en nom d'una persona física o jurídica a la qual representa.
- **Creador d'un segell:** Persona jurídica que crea un segell electrònic.
- **Verificador:** Entitat, ja sigui una persona física o jurídica, que valida o verifica una signatura electrònica recolzant-se en les condicions exigides per la Política d'Identificació i Signatura concreta per la qual es regeix la plataforma de relació electrònica o el servei concret al que s'estigui 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:** Persona física o jurídica que expedeix certificats electrònics o presta altres serveis en relació amb la signatura electrònica.
- **Emissor i gestor de la política de signatura:** Entitat que s'encarrega de generar i gestionar el document de política de signatura i segell, pel qual s'han de regir el signant, el verificador i els prestadors de serveis en els processos de generació i validació de signatura electrònica.

En aquest document s'utilitzarà el terme 'signatari' tant per referir-se al signatari com al creador d'un segell. En el segon dels casos es tractarà d'una actuació administrativa automatitzada.

5. Certificats digitals i altres identitats digitals

5.1 Certificats admesos

El mecanisme de signatura o de segell electrònic amb certificat digital se sustenta en l'existència d'autoritats de certificació que emeten certificats digitals i permeten comprovar que un certificat concret ha estat correctament emès i que continua sent vàlid en el moment del seu ús, és a dir, quan s'emet una signatura electrònica o un segell de temps.

La relació entre l'Autoritat de Certificació i l'entitat que valida el certificat és una relació que es fonamenta en la confiança: els certificats seran acceptats només en la mesura en què l'entitat que l'ha de validar confiï en l'honestedat de l'Autoritat de Certificació.

La Llei 15/2014, de 16 de setembre, de racionalització del sector públic i altres mesures de reforma administrativa estableix en el seu article 24 que *"Les administracions públiques han d'admetre tots els certificats reconeguts inclosos a la "Llista de confiança de prestadors de serveis de certificació" (TSL) establerts a Espanya, publicada a la seu electrònica del Ministeri d'Indústria, Comerç i Turisme"*.

En conseqüència, l'Ajuntament de Mont-roig del Camp admet tots els certificats digitals emesos pels prestadors de serveis de certificació que hagin realitzat la comunicació prevista en l'article 17 de la Llei 6/2020 al Ministeri d'Assumptes Econòmics i Transformació Digital i que compleixin amb els estàndards de qualitat i nivells de seguretat establerts per l'esmentat Ministeri.

L'Ajuntament de Mont-roig del Camp utilitza la plataforma PSIS del Consorci d'Administració Oberta de Catalunya (en endavant CAOC) per a la validació dels seus certificats i dels certificats de tercers, de manera que l'acceptació efectiva de certificats està condicionada per l'actualització dels serveis d'aquesta plataforma.

5.2 Certificats digitals emprats

Podran utilitzar certificats digitals els treballadors de l'Ajuntament de Mont-roig del Camp que hagin de signar documents digitalment o tenir accés a determinats serveis o aplicacions on es requereixi l'autenticació mitjançant certificat digital.

Addicionalment als anteriors, l'Ajuntament de Mont-roig del Camp s'utilitzaran:

- Certificats de representació de l'Ajuntament de Mont-roig del Camp.
- Certificats de segell electrònic per a l'actuació administrativa automatitzada.

- Certificats de servidor web (pàgina web i Seu electrònica) el que permetrà establir comunicacions xifrades amb els usuaris del servidor web utilitzant la tecnologia SSL o TLS.
- Certificats digitals de servidor i d'aplicacions per a l'intercanvi segur d'informació entre AAPP. Cal assenyalar que, si bé aquests certificats no generen actes jurídics, s'ha considerat oportú incorporar-los a aquesta Política per la seva rellevància.

Els treballadors de l'Ajuntament de Mont-roig del Camp utilitzen certificats digitals de treballador públic i segells electrònics emesos pel Consorci AOC, el qual és un prestador reconegut o qualificat de serveis de certificació.

Respecte els certificats de servidor o pàgina web, l'Ajuntament pot utilitzar diferents certificats digitals de diferents prestadors de serveis de certificació. L'ús del certificat està condicionat en cada moment pel nivell d'instal·lació de les claus públiques d'aquests prestadors en els navegadors utilitzats pels ciutadans.

No obstant això, l'Ajuntament podrà utilitzar certificats digitals emesos per altres prestadors en atenció a requeriments específics que puguin existir per a la relació de l'Ajuntament amb altres administracions públiques.

Pel que fa l'ús dels certificats digitals en el servidor per a l'intercanvi segur d'informació entre AAPP, s'utilitzen els del CAOC o qualsevol dels emesos per altres autoritats de certificació que ja tinguin un alt nivell d'instal·lació de les seves claus públiques en els navegadors.

5.3 Altres identitats digitals admeses

En virtut de l'article 9.2 de la Llei 39/2015, l'Ajuntament de Mont-roig del Camp admet com a sistema d'identificació electrònica els diferents sistemes d'identitat digital validats o previstos de ser validats a través de les plataformes VÀLid del CAOC i VALIDe de la Administración General del Estado.

De la mateixa manera que en el cas dels certificats digitals, per a cada procediment administratiu de l'Ajuntament, en base al nivell de seguretat que requereixi aquest, així com el rol amb el que actuï el titular d'aquesta identitat digital, ha de decidir quins sistemes d'identificació es poden utilitzar. L'Ajuntament determinarà, amb caràcter previ a la seva posada en marxa, el nivell de seguretat mínim de la identificació electrònica requerida per a cada tràmit, de cada procediment administratiu que vagi a prestar de forma electrònica, d'acord amb els nivells de seguretat establerts al Reglament eIDAS, tal i com es recull a l'apartat 8.

6. Cicle de vida dels certificats digitals proporcionats

L'Ajuntament de Mont-roig del Camp utilitza com a prestador de serveis de certificació de referència el CAOC i la seva infraestructura de clau pública, utilitzant com a Entitat de Registre el propi Ajuntament. No obstant, atenent a requeriments puntuals es podran utilitzar els serveis d'una altra Autoritat de Certificació.

Serà el CAOC o l'Autoritat de Certificació corresponent la responsable de definir les polítiques de gestió dels certificats digitals que emet i, per tant, qui defineix la vigència dels certificats, la manera com es revoquen, es renoven, es validen, etc.

S'han establert procediments interns que identifiquen les activitats que es realitzen i els seus responsables, així com els procediments a seguir pels usuaris per a la sol·licitud, renovació, revocació, etc. dels seus certificats digitals.

Els certificats digitals emprats seran en qualsevol cas reconeguts i s'emmagatzemaran tant en programari, amb capacitat de generar signatura avançada, com en maquinari, amb capacitat de generar signatura reconeguda mitjançant un dispositiu segur de creació de la signatura que garanteixi que l'ús del certificat digital està sota el control exclusiu de seu titular.

Els certificats digitals basats en suport maquinari es podran emmagatzemar tant en targetes criptogràfiques com en un servidor centralitzat sempre que actuïn com a dispositiu segur de creació de signatura electrònica. El servidor centralitzat haurà de ser operat per un prestador de serveis de confiança per garantir així el compliment de la normativa i estàndards a nivell europeu en matèria de signatura electrònica.

6.1 Certificats digitals de treballadors públics

Els certificats digitals de treballador públic de l'Ajuntament s'emeten i es revoquen en funció de les necessitats del lloc de treball i la seva gestió correspon als Serveis de Tecnologies de la Informació de l'Ajuntament, d'acord amb les particularitats de les Autoritats de Certificació emissores dels certificats electrònics, requerint-se la personació del titular del certificat davant de l'Entitat de Registre de l'Autoritat de Certificació segons aquesta determini.

En el cas dels treballadors de l'Ajuntament, la sol·licitud es genera per part del responsable del servei o departament al que pertany el treballador que requereix de certificat digital, i els Serveis de Tecnologies comproven la vinculació de la persona com a treballador de l'Ajuntament mitjançant certificació emesa per la Secretaria General.

En el cas de treballadors de les entitats dependents de l'Ajuntament, la sol·licitud és realitzada per part de les persones que designarà cada entitat mitjançant instruccions internes i s'actuarà per part dels Serveis de Tecnologies de forma equivalent al que es detalla al paràgraf anterior.

Si el certificat digital és de treballador públic amb càrrec s'acompanyarà la sol·licitud amb una certificació per part del Responsable de la Secretaria General de l'Ajuntament en la qual se certifiqui el càrrec de la persona que sol·licita el certificat.

En cas que un treballador de l'Ajuntament o d'una entitat dependent tingui una incidència com, per exemple, la pèrdua del certificat, aquest haurà de sol·licitar-ne la revocació directament a l'Autoritat de Certificació emissora del certificat digital i posar-ho en coneixement del responsable del seu servei o departament qui a la vegada ho comunicarà a Serveis de Tecnologies .

El Departament de Serveis de Tecnologies durà un control de l'inventari dels certificats que disposa cada entitat. Aquest inventari de certificats digitals es mantindrà actualitzat a partir de la informació de sol·licituds, renovacions i revocacions de certificats digitals.

L'inventari inclourà per a cada certificat digital emès en el marc de les activitats de l'Ajuntament la informació necessària per a la seva gestió com el tipus de certificat, el seu emissor, la persona o aplicació que el gestiona o la seva data de caducitat, entre d'altres dades.

Periòdicament, el Departament de Tecnologies realitzarà un control proactiu de l'inventari de certificats electrònics de forma coordinada amb el Responsable de la Secretaria General per a procedir a la revocació de certificats resultants de canvis de càrrecs dels treballadors o baixes d'aquests.

Amb caràcter previ a la caducitat d'un certificat digital, el seu titular rebrà un correu electrònic des de l'Autoritat de Certificació corresponent, informant de la seva pròxima caducitat. L'usuari haurà de comunicar-ho als Serveis de Tecnologies perquè faci una nova sol·licitud per a la seva renovació seguint el mateix procediment establert per a la sol·licitud d'un nou certificat digital, sempre i quan aquesta renovació no pugui practicar-se de forma directa amb l'Autoritat de Certificació, cas en què s'informarà igualment als Serveis de Tecnologies de la renovació. En cas de no realitzar cap actuació el certificat digital caduca sense que pugui utilitzar-se.

Finalment, els certificats de representant de persona jurídica són assignats als treballadors públics que els requereixen per a l'acompliment de les seves funcions mitjançant la corresponent autorització per part de la Secretaria General que en limiti els usos que es podran donar a aquests certificats. Serveis de Tecnologies portarà un control de la caducitat d'aquests certificats i les seves assignacions als treballadors públics de l'Ajuntament per garantir que siguin mantinguts en el temps aquells que siguin requerits, així com s'estiguin utilitzant per les persones autoritzades per als usos autoritzats.

6.2 Certificats digitals de segell electrònic

En el cas dels certificats de segell electrònic (atribuït a un òrgan) i altres certificats tècnics, el procés de sol·licitud és el següent: l'àrea de l'Ajuntament o l'entitat que en depèn que

necessita d'aquest tipus de certificats els sol·licita als Serveis de Tecnologies de l'Ajuntament, que és qui realitza efectivament la sol·licitud i la descàrrega del certificat digital, per a la seva instal·lació en el servidor i en les aplicacions corresponents. En el cas dels segells electrònics (atribuïts a un òrgan) i de Seu electrònica es requereix també una autorització per part de Secretaria General.

Els segells electrònics d'òrgan per a l'actuació administrativa automatitzada són diferents per a cada servei o unitat de l'Ajuntament, motiu pel qual, cadascuna haurà de disposar del seu segell electrònic, en virtut del que estableix l'article 40 de la Llei 40/2015 i els articles 19 i 20 del Reial Decret 203/2021.

En aquest cas, és el Servei de Tecnologies qui porta un inventari dels certificats de segell electrònic de l'Ajuntament. L'inventari de certificats digitals inclou la informació necessària per a la seva gestió com el tipus de certificat, el seu emissor, l'aplicació que el gestiona, així com la data de la seva caducitat, entre altres.

En el moment en què el Servei de Tecnologies detecta que un certificat inclòs a l'inventari està a punt de caducar, conjuntament amb el sol·licitant del certificat digital i tenint en compte si aquest segell és un dels emprats per a una actuació administrativa automatitzada, decideixen si el certificat ha de renovar-se o no.

En el cas que es decideixi renovar-lo, Serveis de Tecnologies inicia el tràmit de renovació del certificat digital, seguint els mateixos procediments establerts per a la sol·licitud d'un nou certificat digital de segell electrònic. En el cas de segells d'òrgan i de seu electrònica es requereix també una autorització per part de la Secretaria General.

7. Segell de temps

Les característiques principals del segell de temps són:

- El segell de temps és un segell electrònic generat per un tercer de confiança en base a un certificat digital especialment destinat a aquest efecte.
- Evidència de la data i hora en què s'ha produït un acte. S'utilitza conjuntament amb un document en qualsevol format i pot estar signat electrònicament. El segell de temps pot fer referència a:
    - La signatura del document: el segell de temps està associat a la signatura electrònica.
    - Al moment de creació del document: el segell de temps està associat al document.
- Mitjançant un proveïdor de segellat de temps se segellarà la data i l'hora de l'instant en què s'ha realitzat l'acte. El proveïdor serà el proveïdor de serveis de certificació de referència.
- El proveïdor principal del segellat de temps és el Consorci d'Administració Oberta de Catalunya (CAOC) a través de la plataforma PSIS.
- El procés consisteix en crear una evidència electrònica sobre una signatura electrònica: es calcula el resum criptogràfic del document i/o de les seves signatures electròniques (en el cas del ressegellat), és a dir, es realitza una operació matemàtica que s'aplica al conjunt d'informació sobre la qual emetre el segell de temps i s'obté una cadena de bits anomenada "resum criptogràfic" o "hash", la qual es xifra amb la clau privada del certificat de segell de temps utilitzat per fer l'operació. Es retorna aquesta signatura conjuntament amb la data i l'hora de l'operació, així com informació sobre el certificat de segell de temps utilitzat per fer la signatura.
- En cas que sigui necessari generar un segell de temps i el proveïdor no estigui proporcionant el servei, la signatura es generarà sense segell de temps i la data serà la dels servidors de l'Ajuntament. Aquest cas, diferent del cas explicat en els punts anteriors rebrà el nom de «Marca de temps». Els servidors de l'Ajuntament estan sincronitzats a nivell de temps amb l'organisme nacional encarregat de determinar el patró de temps.

8. Nivells de seguretat dels sistemes d'identificació i signatura

En el context de la identificació i l'autenticació per mitjans electrònics, a més de la generació de signatures electròniques, esdevé imperiós afermar la seguretat d'aquests processos. Per aquest motiu, i partint de la regulació que en fa el Reglament Europeu (UE) 910/2014 (ReIDAS) en l'article 8 respecte dels sistemes d'identificació, a continuació s'estipulen els diferents nivells de seguretat en relació als processos d'identificació, autentificació i signatura electrònics.

8.1 Nivells de seguretat d'identificació i autenticació

Segons recull el ReIDAS, la identificació electrònica correspon al procés d'emprar les dades identificatives d'una persona en format electrònic que representen de manera única a una persona física o jurídica, o bé a una persona física que representa a una persona jurídica. L'autenticació, en canvi, és el procés que permet la identificació electrònica d'una persona física o jurídica, o de l'origen i integritat d'unes dades en format electrònica.

En conseqüència, s'estableixen tres nivells de seguretat, segons l'ús que es faci dels mecanismes d'identificació i el grau de confiança que duen associat, en relació amb la identificació i autenticació electròniques:

- **Nivell de seguretat baix:** aquells sistemes d'identificació electrònica que estableixen un grau limitat de confiança sobre la identitat declarada de la persona amb l'objectiu de reduir el risc d'ús indegut o alteració de la identitat presentada.
- **Nivell de seguretat substancial:** aquells sistemes d'identificació electrònica que estableixen un grau substancial de confiança sobre la identitat declarada de la persona amb l'objectiu de reduir substancialment el risc d'ús indegut o alteració de la identitat.
- **Nivell de seguretat alt:** aquells sistemes d'identificació electrònica que estableixen un grau de confiança superior al mitjà d'identificació electrònica amb un nivell de seguretat substancial sobre la identitat declarada de la persona, amb l'objectiu d'evitar l'ús indegut o alteració de la identitat.

Els criteris de classificació per a tot sistema d'identificació electrònica, d'acord amb els nivells de seguretat definits al ReIDAS, s'estableixen en el Reglament d'Execució de la Comissió Europea 2015/1502, de 8 de setembre de 2015.

D'acord amb l'establert al ReIDAS, els nivells de seguretat definits en aquest apartat no són aplicables als sistemes de signatura electrònica.

8.2 Nivells de seguretat de signatura

D'acord amb el capítol III, secció 4a del ReIDAS, els sistemes de signatura electrònica són classificats com a serveis de confiança i, per tant, són susceptibles de ser auditats i qualificats.

En la present política d'identificació i signatura s'estableixen les següents categories per a signatures i segells d'acord amb el marc que defineix el ReIDAS:

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

El Reglament eIdAS defineix la signatura electrònica com les dades en format electrònic annexades a altres dades o associades amb aquestes de manera lògica que empra el signatari per signar, mentre que el segell electrònic és un mecanisme que garanteix l'origen i la integritat d'unes dades. Així doncs, qualsevol mecanisme que encaixi amb aquestes característiques se circumscriuria dins de la primera categoria.

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

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

La tercera categoria correspondria a la de les signatures i segells generats emprant certificats digitals emesos per un Prestador de Serveis de Certificació qualificat, mentre que la quarta referiria a les signatures i segells generats emprant dispositius segurs de creació de signatura i segell.

9. Sistemes d'identificació

En aquest apartat es recopilen i defineixen els diferents sistemes per a la identificació electrònica de les persones que es relacionen amb l'Ajuntament d'acord amb el marc jurídic vigent, en aquest sentit, es podran utilitzar els següents sistemes:

9.1 Sistema d'identificació i signatura basat en número de referència

Mitjançant sol·licitud per part del ciutadà o bé d'ofici per part de l'administració, el ciutadà rep un número de referència que li permetrà identificar-se i realitzar tràmits i altres actuacions vinculades especialment amb el pagament de taxes i preus públics amb l'Ajuntament a través de mitjans electrònics.

El ciutadà rebrà una sol·licitud per a poder utilitzar aquest sistema d'identificació que requereix la verificació de la identitat del sol·licitant.

El número de referència, que s'associa de forma exclusiva a la identitat del ciutadà i únicament pels tràmits i actuacions pels quals s'ha habilitat, es genera de forma automàtica en un entorn segur mitjançant un algorisme que relaciona dades del ciutadà i del tràmit o actuació i té una longitud fixa específica de caràcters alfanumèrics i pot ser emmagatzemat en els sistemes informàtics de l'Ajuntament.

La comunicació al ciutadà d'aquest número de referència es practicarà a través d'un canal segur, ja sigui per via electrònica, postal, presencial o telefònica. En aquesta comunicació també s'informarà a l'interessat sobre les condicions d'ús d'aquest sistema. Així s'assegura la confidencialitat i l'autenticitat mitjançant el coneixement exclusiu per part del ciutadà i de l'Ajuntament del número de referència.

El número de referència té associat un període de validesa i un cop finalitzat el mateix deixa d'estar operatiu. Això suposa la impossibilitat de realitzar tràmits o actuacions amb el citat número de referència. Altrament, el ciutadà podrà sol·licitar l'extinció del número de referència, la qual cosa també implica la impossibilitat de realitzar tràmits o actuacions amb aquest número.

En cas que l'actuació realitzada pel ciutadà comporti la presentació de documents electrònics utilitzant el mecanisme descrit en aquest punt com a sistema de signatura electrònica, l'Ajuntament generarà automàticament un acusament de rebuda de la seva presentació.

La utilització del sistema descrit implicarà el consentiment per part del ciutadà per al seu ús com a sistema de signatura electrònica.

D'acord al que estableix el Reglament eIDAS, el nivell de seguretat d'aquest sistema d'identificació electrònica és baix.

9.2 Sistema d'identificació i signatura amb informació coneguda pel ciutadà i l'Ajuntament

Mitjançant aquest sistema d'identificació que permetrà al ciutadà identificar-se i realitzar determinats tràmits i actuacions que no impliquin accés o consulta de dades personals, més enllà dels propis del procediment i les dades d'identificació de l'interessat, el ciutadà aportarà un seguit de dades conegudes, de forma raonable, únicament per ell i l'Ajuntament. Així s'assegura la confidencialitat i l'autenticitat mitjançant el coneixement exclusiu per part del ciutadà i de l'Ajuntament del número de referència.

També es considerarà el temps de validesa, que serà temporal, d'aquestes dades per les quals es dona accés al sistema.

En cas que l'actuació realitzada pel ciutadà comporti la presentació de documents electrònics utilitzant el mecanisme descrit en aquest punt, com a sistema de signatura electrònica, l'Ajuntament generarà automàticament un acusament de rebuda de la seva presentació.

La utilització del sistema descrit implicarà el consentiment per part del ciutadà per al seu ús com a sistema de signatura electrònica.

D'acord al que estableix el Reglament eIDAS, el nivell de seguretat d'aquest sistema d'identificació electrònica és baix.

9.3 Sistema basat en contrasenyes d'un sol ús lliurades a través d'un dispositiu electrònic a un usuari prèviament enregistrat

El sistema es basa en la confirmació de la identitat d'una persona mitjançant un registre d'usuaris que l'Ajuntament ha de posar a disposició del ciutadà al qual s'ha d'inscriure per a tenir accés al sistema que proporciona contrasenyes d'un sol ús i valida la seva identitat. El registre d'usuaris proporcionat per l'Ajuntament, per l'Administració de la Generalitat de Catalunya o per l'Administració General de l'Estat disposa d'un nivell de seguretat substancial o superior d'acord amb el Reglament eIDAS i sempre que hi hagi una comprovació de la identitat del ciutadà d'acord al que s'estipula a l'article 2.1.2. de l'Annex del Reglament d'Execució de la Comissió Europea 2015/1502, de 8 de setembre de 2015 per a aquest nivell de seguretat.

El ciutadà inscrit al registre d'usuaris associa a la seva persona un identificatiu d'un dispositiu electrònic, és a dir, se li proporcionarà un codi d'usuari per a poder sol·licitar a través del

sistema d'identificació una clau d'un sol ús. El sistema d'identificació de l'Ajuntament generarà i enviarà al dispositiu electrònic la contrasenya d'un sol ús per a l'usuari introduït. Per mitjà de les dades identificatives proporcionades, el ciutadà podrà accedir als tràmits i actuacions que han estat habilitats en relació en aquest sistema i que no impliquin accés o consulta de dades personals més enllà dels propis del procediment i les dades d'identificació de l'interessat.

La validesa del sistema podrà estar limitada temporalment en funció dels terminis associats als tràmits o actuacions per els que s'hagi determinat la seva utilització.

La utilització del sistema descrit implicarà el consentiment per part del ciutadà per al seu ús com a sistema de signatura electrònica.

D'acord al que estableix el Reglament eIDAS, el nivell de seguretat d'aquest sistema d'identificació electrònica és alt.

La confidencialitat i l'autenticitat es garanteixen mitjançant el coneixement exclusiu per part del ciutadà i de l'Ajuntament de les dades proporcionades pel ciutadà al formulari de registre, l'usuari i paraula d'accés per a duu a terme la signatura.

9.4 Sistema basat en certificats electrònics

L'Ajuntament, en aquesta Política, preveu els següents escenaris d'us mitjançant el sistema basat en certificats electrònics:

- **Signatura electrònica:** l'autenticació, no repudi i la integritat dels documents i continguts amb independència de la transmissió dels mateixos per mitjans telemàtics.
- **Autenticació:** permet l'autenticació de la persona física o jurídica als diferents serveis de l'administració electrònica mitjançant credencials.
- **Xifratge de dades:** la transmissió de dades proporciona seguretat en l'intercanvi de dades per mitjà de la garantia de l'autenticació, no repudi i la integritat del missatge.

9.5 Mecanismes d'identificació

A continuació, es llisten les diferents tipologies de certificats i mitjans d'identificació acceptats per l'Ajuntament de Mont-roig del Camp per a la identificació i l'autenticació de ciutadans, empreses, treballadors públics i ens de l'administració pública.

9.5.1 Per a ciutadans

- Els certificats electrònics qualificats que hagin estat emesos per Prestadors de Serveis de Certificació (PSCs) inclosos a la Trusted Services List (TSL) publicada per l'òrgan competent de qualsevol país de la Unió Europea d'acord amb el que estableix el ReIdAS.
- S'hauran d'admetre, amb caràcter general, qualsevol dels mitjans d'identificació inclosos a la llista que publicarà la Comissió Europea, per accedir als serveis prestats en línia per un organisme del sector públic en un Estat Membre, a efectes de l'autenticació transfronterera, conforme al que estableix el mateix reglament.
- Els certificats qualificats reconeguts de signatura qualificada i/o avançada, com l'idCAT per a ciutadà que emet el Consorci AOC, el DNI electrònic o d'altres expedits per prestadors inclosos en les Llistes de confiança de prestadors de serveis de certificació de l'Administració General de l'Estat.
- Els mecanismes d'identificació i signatura electrònica dels ciutadans (persones físiques) no criptogràfics basats en l'enviament de paraules de pas i/o codis d'un sol us a dispositius mòbils, com el sistema Cl@ve de l'AGE (Cl@ve PIN, Cl@ve Permanente i Cl@ve Firma) o l'IdCAT-Mòbil del Servei VÀLid del Consorci AOC.

9.5.2 Per a empreses

- Els certificats reconeguts emesos a una persona jurídica o a un ens sense personalitat i custodiats per una persona física, titular del certificat, la qual el pot emprar per actuar en nom de l'empresa o de l'ens indicat al certificat.
- Els certificats reconeguts emesos a una persona jurídica o a un ens sense personalitat, amb indicació expressa de la representació que ostenta la persona física titular del certificat.
- Els certificats de segell electrònic qualificat emesos a una persona jurídica o a un ens sense personalitat per Prestadors de Serveis de Certificació (PSCs) inclosos a la Trusted Services List (TSL) publicada per l'òrgan competent de qualsevol país de la Unió Europea d'acord amb el que estableix el ReIdAS.
- També els mecanismes indicats per a la identificació de persones físiques, quan s'emprin per autenticar la identitat d'un ciutadà que declara representar a una persona jurídica. Quan s'escaigui, aquesta representació es podrà verificar mitjançant la consulta a un registre en línia de representacions; especialment, mitjançant el servei REPRESENTA del Consorci AOC, les condicions del qual es publiquen a la seva web.

9.5.3 Per a treballadors públics

- El certificat reconegut o qualificat que el Consorci AOC emet als treballadors del Sector Públic de Catalunya en dispositiu segur de creació de signatura: la T-CAT.
- El certificat reconegut o qualificat que el Consorci AOC emet als treballadors del Sector Públic de Catalunya en suport programari: la T-CAT P.
- Els certificats reconeguts o qualificats emesos per prestadors inclosos a la “Llista de confiança de Prestadors de Serveis de Certificació (TSL)” publicada pel Ministerio de Industria, Comercio y Turismo conforme al perfil "Empleado público" aprovat pel Consejo Superior de Administración Electrónica.
- Qualsevol perfil de certificats reconeguts o qualificats emesos per prestadors inclosos a la “Llista de confiança de Prestadors de Serveis de Certificació (TSL)” publicada pel Ministerio de Industria, Comercio y Turismo que acreditin la vinculació del seu titular a un ens públic.

9.5.4 Pels ens de l’administració

- Els certificats qualificats de seu electrònica i de servidor segur que el Consorci AOC emet als ens del Sector Públic de Catalunya.
- Els certificats electrònics qualificats emesos per altres Prestadors de Serveis de Certificació - diferents al Consorci AOC - inclosos a la Trusted Services List (TSL) del Ministerio de Industria, Comercio y Turismo conforme al perfil "Sede electrónica administrativa" aprovat pel Consejo Superior de Administración Electrónica.
- D’altres certificats qualificats d’autenticació de lloc web, d’acord al que estableix l’Article 45 de ReIdAS, emesos a nom d’un ens.

10. Sistemes, classes, tipologies i nivells de signatura o segell electrònic

En aquest apartat es recopilen els aspectes relacionats amb la signatura electrònica en el marc de l'Ajuntament de Mont-roig del Camp, incloent els diferents usos de la signatura electrònica i del segell electrònic en l'àmbit dels seus sistemes. Els objectius que persegueix amb la implantació de la signatura electrònica són fonamentalment els següents:

- Dotar-se d'un sistema per al control, l'ús i la conservació de la documentació original signada electrònicament i gestionada en el desenvolupament habitual de la seva activitat política i administrativa.
- Garantir la gestió adequada dels documents electrònics, assegurant-ne l'autenticitat, fiabilitat, integritat i disponibilitat futura al llarg del seu cicle de vida.
- Donar resposta a les exigències en matèria d'arxiu electrònic de la Llei 39/2015 i de l'Esquema Nacional d'Interoperabilitat.

Un cop formulats aquests objectius bàsics, cal tenir presents les definicions dels diferents sistemes de signatura electrònica existents, on l'Ajuntament podrà utilitzar les següents tipologies de signatura electrònica:

- **Signatura electrònica bàsica (no criptogràfica):** Entenent la signatura electrònica com aquelles dades en format electrònic annexades a altres dades electròniques o associades de manera lògica amb aquestes que utilitza el signant per signar, la signatura electrònica bàsica és el sistema de signatura més senzill, que permet identificar digitalment el signant amb les seves dades, però oferint un baix nivell de seguretat.
- **Signatura electrònica basada en l'ús d'un certificat digital:** Aquest és el sistema de signatura electrònica en el qual, d'acord amb la clau privada d'un usuari, es xifra el resum criptogràfic del document i de la signatura i s'afegeix sobre la signatura informació sobre el certificat utilitzat per a la signatura, la data de la signatura, la política de signatura emprada, etc.
- **Signatura electrònica basada en la identificació més les evidències de la voluntat de la signatura:** Aquest sistema consisteix en la identificació d'un usuari a partir d'un usuari i contrasenya (o una paraula de pas personal, o un número de referència compartit únicament entre l'usuari i l'Ajuntament) i, en el moment de signar un document, la captura de les evidències de l'autenticació d'aquesta persona més el resum criptogràfic del document a signar, l'hora i la data de la signatura i la incorporació d'aquestes evidències al document i la seva signatura amb un segell electrònic de l'Ajuntament completada amb segell de temps. Aquest sistema també serà d'aplicació per a aquells sistemes de signatura que permetin l'ús d'un PIN d'un sol ús enviat a un

número de telèfon mòbil o a un correu electrònic cas en que s'incorporaran les evidències de l'ús correcte del PIN i la correspondència entre el PIN enviat i l'introduït pel signatari.

- **Signatura biomètrica.** Aquest sistema consisteix en l'adquisició de les evidències biomètriques del signant, així com del context de la signatura ("hash" del document, moment de la signatura, coordenades GPS, etc.) en un dispositiu especialitzat. Aquesta informació és xifrada amb una clau privada que està custodiada per un tercer de confiança (per exemple, un notari) i s'emmagatzema o bé en el mateix document signat o bé en un repositori de signatures.

  La validació de les signatures s'efectua en el moment que una signatura sigui posada en dubte. En aquest moment, l'Ajuntament aportarà davant de l'autoritat que hagi de dirimir el litigi el document, així com la seva signatura (evidències xifrades), i serà aquesta qui ha de sol·licitar el desxifrat de les evidències al tercer de confiança i, a partir d'aquestes evidències i del resum criptogràfic del document, es podrà provar la identitat del signant, la integritat del document i la vinculació de la signatura amb el document.

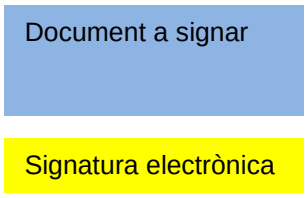
Des del punt de vista jurídic, les signatures electròniques poden ser:

- **Simple o ordinària**: És el conjunt de dades en forma electrònica que, consignades conjuntament amb altres o que estan associades, poden ser utilitzades com a mitjà d'identificació del signant. La identificació s'ha d'entendre com l'autenticació d'entitats, segons el que estableix el Reglament Europeu (UE) 910/2014 relatiu a la identificació electrònica i els serveis de confiança en les transaccions electròniques.
- **Signatura electrònica avançada**: És la signatura electrònica que permet identificar el signant i detectar qualsevol canvi posterior de les dades signades que està vinculada al signant de manera única i a les dades a què fa referència i que ha estat creada per mitjans que el signant pot mantenir sota el seu control exclusiu.
- **Signatura electrònica reconeguda o qualificada**: És la signatura electrònica avançada que es basa en un certificat reconegut o qualificat i que ha estat generada mitjançant un dispositiu segur de creació de signatura, segons estableix l'article 3, 12) del Reglament Europeu (UE) 910/2014 relatiu a la identificació electrònica i els serveis de confiança en les transaccions electròniques en el mercat interior.

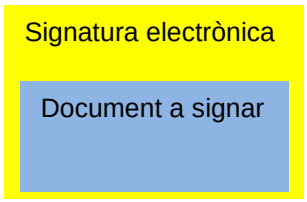
Per a les definicions anteriors s'utilitza el concepte clau de **certificat reconegut o qualificat**, que segons el Reglament (UE) 910/2014, en el seu article 3, 15), el defineix com *un certificat de signatura electrònica que ha estat expedit per un prestador qualificat de serveis de confiança i que compleix els requisits establerts en l'annex 1* del Reglament.

A continuació, es presenten les definicions de **tipus de signatura** des d'un punt de vista tècnic:

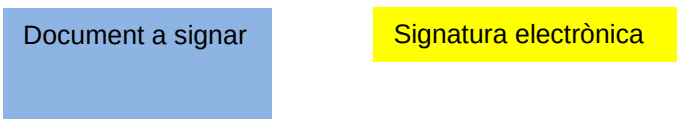
- **Signatura attached**: Les dades de signatura es localitzen en el document signat. Per tant, el mateix document disposa de tota la informació per comprovar l'autenticitat i la integritat del document, així com la informació necessària per a la validació de la signatura. Cal diferenciar entre dos tipus diferents de signatura attached:
    - **Enveloped (incrustada):** El document signat està compost pel contingut del document a signar més la signatura d'aquest contingut.



    - **Enveloping (envoltant):** El document signat és la signatura electrònica del document a signar i dins d'aquesta signatura hi ha el mateix document a signar.



- **Signatura detached**: Les dades de signatura es localitzen fora del document a signar, però es troben associades a aquest. Les dades de la signatura es mantenen per separat durant tot el cicle de vida del document. Per validar la signatura cal crear un document d'evidència electrònica que contingui de forma conjunta el document i les seves dades completes de la signatura.

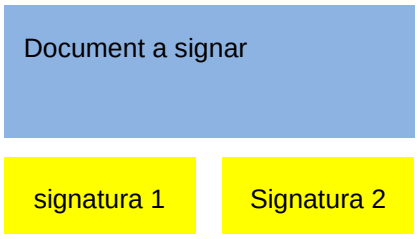


A continuació, es defineixen els diferents nivells de signatura electrònica:

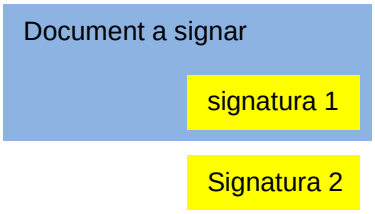
- **Signatura simple**: el document conté una única signatura.
- **Signatura múltiple**: el document conté dues o més signatures. Aquesta signatura múltiple consisteix en què diversos signants signin el document consecutivament.

Aquesta signatura es pot aplicar sobre el document original cada vegada, que és el que s'identifica com a signatura paral·lela, o sobre el document signat, que és el que s'identifica com a signatura niuada.

Document signat amb signatura paral·lela:



Document signat amb signatura niuada:



La signatura múltiple es pot utilitzar en diverses situacions en el marc dels procediments de l'Ajuntament de Mont-roig del Camp com, per exemple, en la signatura de documents electrònics per part de més d'una persona.

10.1 Formats de signatura

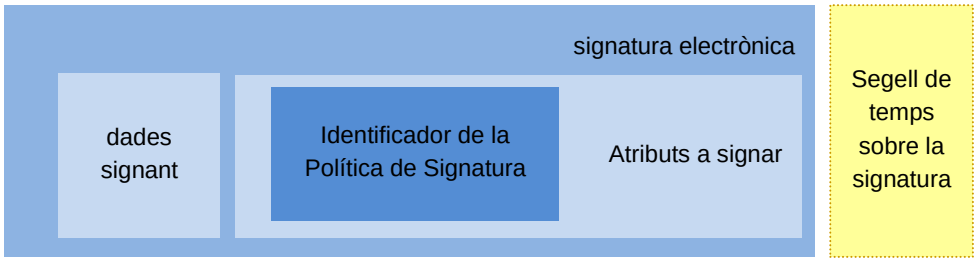
Partint dels conceptes bàsics sobre signatura electrònica descrits anteriorment, a continuació es descriuen els formats de signatura electrònica que utilitzarà l'Ajuntament de Mont-roig del Camp en el marc de la present Política d'Identificació i Signatura Electrònica.

10.1.1 Signatura electrònica amb Política d'Identificació i Signatura Electrònica i segell de temps

Aquest serà el format de signatura electrònica, tant avançada com reconeguda, per als documents electrònics que s'hagin de guardar al sistema de gestió de documents electrònics de l'Ajuntament de Mont-roig del Camp.

El format de signatura derivat de la signatura electrònica avançada o reconeguda amb identificador de Política amb la incorporació d'un segell de temps que situa la signatura electrònica en un moment determinat del temps és **AdES-T**. La representació gràfica d'aquest format de signatura és la següent:

Signatura electrònica AdES-T



La signatura electrònica amb política explícita (XAdES-T o PAdES-T) ha de contenir tots els elements que es llisten a continuació, dels quals tots, excepte l'últim, corresponen al format XAdES-EPES o PAdES-EPES (signatura electrònica avançada amb identificador de política):

- Les dades signades per l'usuari com, per exemple, un document electrònic.
- El tipus de contingut signat: ContentType.
- El resum criptogràfic del missatge: messageDigest.
- El certificat emprat per signar: ESSSigningCertificate o OtherSigningCertificate.
- La data i hora al·legada de la signatura: signingTime (opcional).
- Les pistes sobre el contingut signat: ContentHints (opcional).
- La identificació del contingut: ContentIdentifier (opcional).
- La referència als continguts: ContentReference (opcional).
- La indicació del tipus de compromís: CommitmentTypeIndication (opcional).
- La localització del signant: SignerLocation (opcional).
- Els atributs del signatari: SignerAttributes (opcional).
- El segell de data i hora sobre el contingut: ContentTimestamp (opcional).
- Contrafirma: Countersignature (opcional).
- Identificació de la Política de signatura: SignaturePolicyIdentifier (definit a la present política com la normativa de signatura electrònica).
- Segell de data i hora de la signatura: SignatureTimeStamp.

Aquest tipus de signatura s'usa per a qualsevol tipus de document que no hagi de conservar-se durant més temps que el temps de validesa del segell de temps corresponent.

Per a documents PDF o PDF/A s'utilitzarà la signatura PAdES amb segell de temps.

Per documents XML (factures electròniques, índex de l'expedient o altres documents rebuts via interoperabilitat) es faran servir signatures XAdES-T, preferiblement attached enveloping.

Per a la resta de documents es faran servir signatures XAdES-T dettached.

10.1.2 Signatura electrònica d'arxiu

Aquest serà el format de signatura electrònica avançada o reconeguda per als documents electrònics i els documents d'índex d'expedients que s'hagin de guardar durant més temps del temps de caducitat del certificat digital utilitzat per generar el segell de temps associat a la signatura electrònica.

En el cas de múltiples signatures es tindran en compte els següents elements:

- **En paral·lel:** primera data de caducitat del segell de temps dins de les diferents signatures.
- **Niuades:** data de caducitat del segell de temps de l'última signatura.

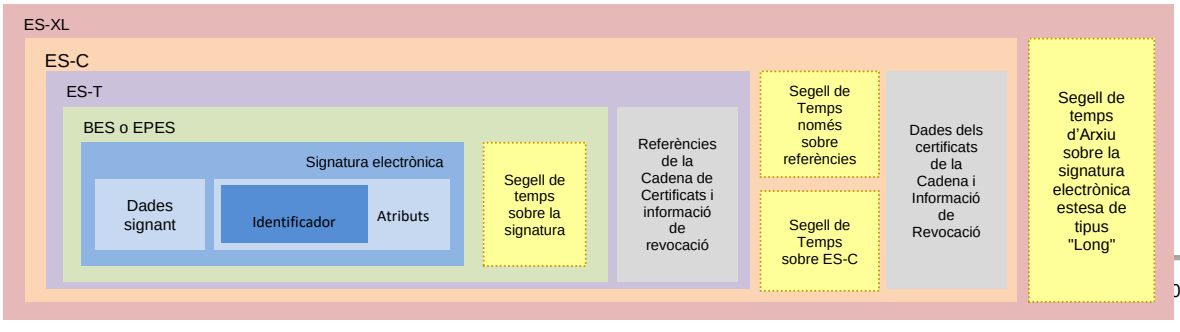
En aquest cas es preveuen dos formats: AdES-A i PAdES-LTV.

El format de signatura derivat de la signatura electrònica avançada o reconeguda amb identificador de Política amb la incorporació d'un segell de temps que situa la signatura electrònica en un moment determinat del temps i amb capacitat d'afegir segells de temps successius per preservar la seva validesa és **AdES-A** o, en el cas de documents en format PDF, **PAdES-LTV**. La representació gràfica d'aquest format de signatura és la següent:

La signatura electrònica d'arxiu (AdES-A) prové del format de signatura electrònica extensa (XL), que inclou tots els elements de verificació de la vigència del certificat per a poder repetir la validació de manera autònoma.

Sobre aquest format extens de signatura s'afegeix un segell de temps, preveient el ressegellat successiu de manera periòdica. Aquest és el format de signatura més complet i està pensat expressament pels documents dels quals es vol garantir la integritat i validesa jurídica al llarg del temps.

Signatura electrònica de Arxiu (ES-A)



- La signatura electrònica XML: Signature
- El certificat utilitzat per a signar: SigningCertificate o KeyInfo:X509Data
- La data i hora al·legada de la signatura: signingTime (opcional)
- El format de l'objecte de dades signat: DataObjectFormat (opcional)
- La indicació del tipus de compromís: CommitmentTypeIndication (opcional)
- El lloc de producció de la signatura: SignatureProductionPlace (opcional)
- El paper del signant: SignerRole (opcional)
- El segell de data i hora sobre el contingut: AllDataObjectsTimeStamp o IndividualDataObjectsTimeStamp (opcional)
- La contrafirma: Reference o CounterSignature (opcional)
- Identificació de la política de signatura: SignaturePolicyIdentifier (definit a la present política com la normativa de signatura electrònica)
- Segell de data i hora de la signatura: SignatureTimeStamp
- Referències completes de certificats: CompleteCertificateRefs
- Referències completes de revocació: CompleteRevocationRefs
- Referències completes de certificats d'atributs: AttributeCertificateRefs
- Referències completes de revocació d'atributs: AttributeRevocationRefs
- Segell de data i hora sobre la signatura completa: SigAndRefsTimeStamp
- Segell de data i hora sobre les referències de certificats i revocacions: RefsOnlyTimeStamp
- Valors de certificats: CertificateValues
- Valors de revocació: RevocationValues
- Valors de certificats d'atribut: AttrAuthoritiesCertsValues
- Valors de revocació de certificats d'atribut: AttributeRevocationValues
- Segell de data i hora d'arxiu: ArchiveTimeStamp

Signatura PAdES-LTV

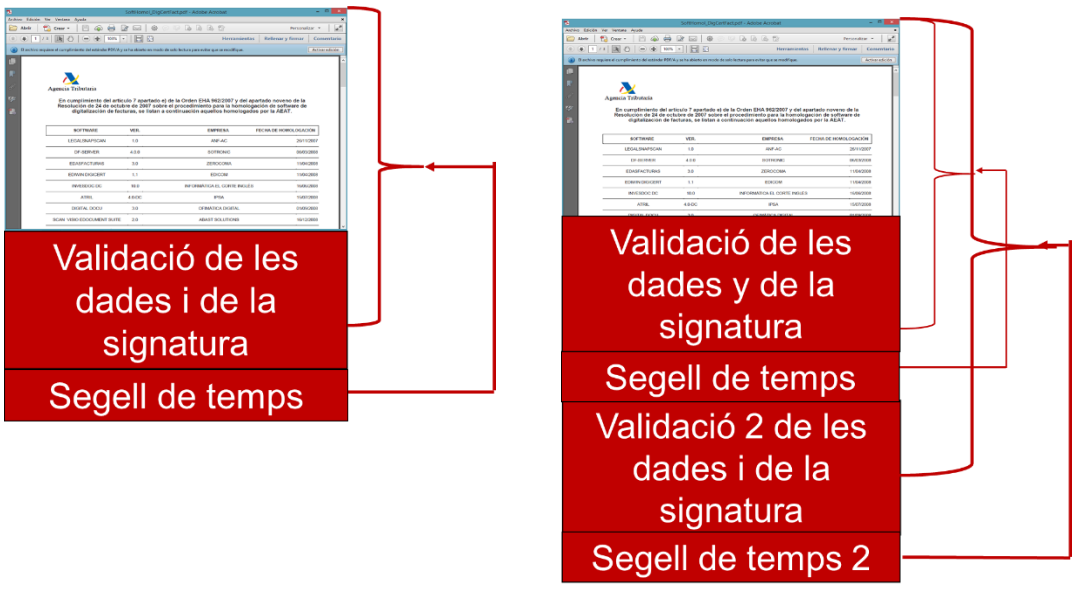
La signatura electrònica de llarga durada (LTV-Long Term Validation) és un format específic de la família PAdES. La signatura més bàsica, la PAdES Basic, està especificada en la ISO 32000-1.

La signatura PAdES-EPES inclou la signatura electrònica del document en format CAdES-BES amb segell de temps (recomanat) i una resposta de validació d'un servei OCSP (recomanat). A més, pot incloure motius de signatura, el lloc de la signatura i dades de contacte del signant. També inclou la Política de Signatura (definida a la present Política com la normativa de signatura electrònica).

Sobre aquestes signatures es pot construir una signatura PAdES-LTV que inclou, per a la verificació de les signatures i del contingut, informació sobre la validesa dels certificats electrònics de les autoritats de certificació en el moment de la validació mitjançant la resposta del servei de validació OCSP i un segell de temps sobre aquesta verificació de signatures.

Posteriorment, es pot afegir a la signatura un nou comprovant de verificació, que garanteix que la verificació que es va fer en el seu moment continua sent vàlida, i s'afegeix un nou segell de temps per a protegir les signatures i les seves validacions.

Exemple:



Aquest tipus de signatura s'usa per a qualsevol tipus de document que hagi de conservar-se durant més temps que el temps de validesa del segell de temps corresponent.

Per a **documents PDF o PDF/A** s'usarà la signatura **PAdES-LTV amb segell de temps**.

Per **documents XML** (factures electròniques, índex de l'expedient o altres documents rebuts via interoperabilitat) es faran servir signatures **XAdES-A**, preferiblement **attached enveloping**.

Per a la **resta de documents** es faran servir signatures **XAdES-A dettached**.

10.1.3 Signatura electrònica a través d'acreditació de la identitat i d'evidències de la voluntat de signatura

Aquest serà un format específic de signatura electrònica avançada pels documents electrònics que signi electrònicament un ciutadà o un treballador públic a partir de l'ús de la identitat basada en l'usuari i contrasenya de l'Ajuntament de Mont-roig del Camp.

El procés de signatura es realitza de la següent manera:

- L'usuari s'haurà acreditat anteriorment en el sistema i constarà en els registres d'aquest.
- L'usuari omplirà el formulari a signar i manifestarà la seva voluntat de signatura mitjançant l'usuari de l'Ajuntament. Això generarà alguna de les següents opcions:
    - Un **e-mail** a una adreça de correu registrada on s'envia un PIN d'un sol ús.
    - Un **SMS** a un telèfon mòbil registrat on s'envia un PIN d'un sol ús.
    - Apareixerà una pantalla on es demanarà a l'usuari que introdueixi una **coordenada de la targeta de claus**.

En tots tres casos, si l'usuari introdueix correctament el PIN o la coordenada, es generarà una evidència electrònica que es guardarà com a metadada del document a signar (signatura primària). A continuació, es procedirà a la signatura del document amb un segell electrònic de l'Ajuntament més un segell de temps (signatura secundària).

Les evidències electròniques que es guarden en aquest tipus de signatura han d'incloure sempre l'identificador de l'usuari que ha signat, la identificació del lloc de treball des del qual s'ha signat (IP), la data i l'hora en què ha signat i el sistema de signatura que ha utilitzat (codi de la targeta de claus o bé PIN enviat al correu electrònic o al SMS).

En aquest format de signatura pot haver-hi més d'una signatura d'aquest tipus sobre el document, i aquestes sempre seran en niades.

La signatura podrà combinar-se amb un altre tipus de signatura basada en certificat digital.

Per tant, la validesa jurídica de la signatura electrònica a través d'acreditació de la identitat i d'evidències de la voluntat està vinculada al document i a les evidències del procés d'identificació del signant amb el PIN enviat al correu electrònic o al mòbil o la coordenada introduïda (signatura primària). Aquestes evidències es guarden com a metadada del document, aportant la signatura electrònica de segell electrònic de l'Ajuntament i el segellat de temps del document signat únicament com a evidències d'integritat i no d'autenticitat (signatura secundària).

Per a l'ús d'aquest tipus de signatura cal una regulació específica, tal i com es requereix a l'article 10 de la Llei 39/2015.

En cas de conflicte, l'Ajuntament ha d'acreditar que ha aprovat i publicat a la Seu Electrònica la regulació específica, que ha generat les evidències no només en aquesta signatura, sinó en qualsevol altra signatura del mateix tipus (signatura primària), que aquesta signatura es va produir en un moment determinat (segell de temps) i que el contingut del document no ha canviat ("hash" signat amb el primer segell electrònic (signatura primària) i document amb la seva signatura signat amb el segon segell electrònic (signatura secundària).

10.1.4 Signatura electrònica biomètrica

Aquest serà un cas específic de signatura electrònica avançada per als documents electrònics que es generen presencialment davant d'un tercer i en els quals es guarda de forma xifrada, conjuntament amb el resum criptogràfic del document, la següent informació:

- Dades biomètriques de la persona que signa de forma manuscrita el document, entre elles:
    - Detall temporal de la realització de la signatura (inici, final i durada en milisegons).
    - Detall de la traça en relació a la velocitat, acceleració i pressió del traç en tota la seva figura.

  Les dades biomètriques es recullen amb elements específics acreditats de captura d'aquesta tipologia de dades, permetent al signant la visualització del document a signar en el mateix acte de signatura.
- Altra informació que pugui resultar rellevant per al procés de signatura o el document signat, com la identificació del programari i maquinari de captura de signatura o la localització GPS de l'element maquinari de captura de signatura.

El xifrat d'informació de la signatura es realitza amb la clau pública d'un certificat digital específic de signatura electrònica biomètrica, que s'emmagatzema en els servidors de l'Ajuntament (o en el mateix dispositiu). La clau privada és custodiada per un tercer de

confiança, a qui se li requerirà quan sigui necessari verificar una signatura biomètrica, per exemple, en cas de reclamació o de litigi.

En aquest format de signatura pot haver més d'una signatura biomètrica sobre el document, però sempre seran en paral·lel.

En qualsevol cas, un cop finalitzades totes les signatures biomètriques i un cop xifrada la informació esmentada anteriorment, es guardarà tot de forma conjunta amb el document i, per garantir la seva integritat, es realitzarà sobre el mateix document una signatura electrònica de segell electrònic d'aplicació pertanyent a l'Ajuntament de Mont-roig del Camp completada amb un segell de temps.

Per tant, la validesa jurídica de la signatura electrònica biomètrica està vinculada al document i a les evidències biomètriques que es guarden dins el mateix document de forma xifrada, mentre que la signatura electrònica i el segellat de temps únicament s'incorporen per a proporcionar les característiques requerides d'integritat, però no d'autenticitat.

En cas de conflicte, un cop desxifrades les dades per part del tercer de confiança que custodia la clau privada del certificat de xifrat, s'haurà de generar un peritatge de les dades biomètriques guardades en el document i comparar-les amb una nova captura de dades biomètriques de la persona a qui suposadament corresponen les dades biomètriques i que s'ha de fer sota condicions similars d'elements maquinari i programari amb les que es va realitzar la signatura a verificar.

En aquest sentit, el tercer de confiança que custodiï la clau privada del certificat digital de xifrat haurà de comptar amb, o se li haurà de proporcionar en el moment del peritatge, un maquinari i programari client de l'aplicació de generació de signatures biomètriques, així com de l'aplicació que permeti el desxifrat en interpretació de les dades biomètriques.

10.2 Mecanismes de signatura i segells electrònic

Amb caràcter general, els mecanismes de signatura que es descriuen en aquest apartat tenen, així mateix, efectes d'identificació dels ciutadans, les empreses, els treballadors públics i els ens de l'Administració.

10.2.1 Per a ciutadans

- Els certificats electrònics que hagin estat emesos per Prestadors de Serveis de Certificació (PSCs) inclosos a la Trusted Services List (TSL) publicada per l'òrgan competent de qualsevol país de la Unió Europea d'acord amb el que estableix el ReIdAS.

- El certificat reconegut o qualificat de signatura avançada IdCAT que emet el Consorci AOC.
- S'hauran d'admetre els certificats del DNI-e, d'acord al que estableix la Llei 39/2015, del Procediment Administratiu Comú de les Administracions Públiques.
- Els mecanismes IdCAT Mòbil o Cl@ve (Cl@ve PIN, Cl@ve Permanente i Cl@ve Firma) com a mecanismes signatura electrònica dels ciutadans (persones físiques) no criptogràfics.

10.2.2 Per a empreses

Les persones jurídiques i els ens sense personalitat jurídica podran fer servir i generar signatures electròniques mitjançant els mecanismes d'identificació especificats en el punt 9.5.1. de la present Política.

10.2.3 Per a treballadors públics

Els treballadors públics podran fer servir i generar signatures electròniques mitjançant els mecanismes d'identificació especificats en el punt 9.5.2. de la present Política.

10.2.4 Pels ens de l'Administració davant dels ciutadans

- Els certificats qualificats de segell electrònic que el Consorci AOC emet als ens del Sector Públic de Catalunya.
- Els certificats reconeguts o qualificats emesos per altres Prestadors de Serveis de Certificació inclosos a la Trusted Services List (TSL) del Ministerio de Industria, Comercio y Turismo conforme al perfil "Sello electrónico" aprovat pel Consejo Superior de Administración Electrónica.
- En l'àmbit de l'actuació administrativa automatitzada, d'acord al que disposa la Llei 40/2015, de l'1 d'octubre, de Règim Jurídic del Sector Públic:
    - El codi segur de verificació (CSV) com a mecanisme de signatura electrònica dels ens en actuació administrativa automatitzada, el qual permet comprovar la integritat del document així signat mitjançant la consulta de l'original a la seu electrònica corresponent.
    - Els certificats reconeguts o qualificats de segell electrònic que el Consorci AOC emet als ens del Sector Públic de Catalunya.

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

10.3 Validació de signatures o segells

Per garantir la validesa jurídica dels documents electrònics signats digitalment, qualsevol document que entri o es generi a l'Ajuntament i que contingui una signatura o segell electrònic i/o un segell de temps, prèviament al seu emmagatzematge al gestor documental, cal validar-lo.

Per a validar-lo s'utilitzarà algun d'aquests sistemes:

- La plataforma de validació PSIS del CAOC i els procediments que aquesta estableixi en cada moment.
- Mitjançant el procés abans especificat per a les signatures a través d'acreditació de la identitat i d'evidències de la voluntat de signatura.
- Mitjançant el procés abans especificat per a les signatures electròniques biomètriques.

Per a les signatures electròniques avançades i reconegudes, només en aquells casos en què el procés de validació de totes les signatures electròniques i dels segells electrònics sigui satisfactori, es procedirà a emmagatzemar el document electrònic dins del gestor documental.

Per a les signatures a través d'acreditació de la identitat i d'evidències de la voluntat de signatura i biomètriques, es procedirà a emmagatzemar el document electrònic amb les seves signatures al gestor documental directament, sense cap validació addicional, ja que els sistemes de signatura d'aquest tipus són segurs i no compten amb un procés automatitzat de validació.

11. Manteniment i preservació de les signatures i dels segells electrònics

La signatura o segell electrònic atorga validesa jurídica als documents electrònics. No obstant això, aquesta validesa està subjecta a certs riscos que s'han de gestionar degudament, per tal de mantenir aquesta validesa jurídica del document en suport electrònic, de forma indefinida en el temps. Aquests riscos són els següents:

1. **Caducitat o revocació del certificat digital amb el qual se signa un document electrònic.** Pot qüestionar-se la validesa d'un document electrònic a partir del dia de la caducitat del certificat digital si no es pot acreditar amb total garantia la data en què es va generar aquesta signatura, la qual ha de ser, evidentment, posterior a la data d'emissió del certificat digital i anterior a la data de revocació o caducitat del certificat digital.

   Per a garantir el moment en què es va generar la signatura electrònica, aquesta es completarà amb un segell de temps emès per una Autoritat de Temps. Per tant, per a evitar aquest risc, es realitzaran signatures AdES-T.

2. **Validesa del certificat digital en el moment de generar-se la signatura electrònica.** Pot qüestionar-se la validesa d'un document electrònic si no hi ha evidència suficient sobre que el certificat digital era vigent el dia que es va generar la signatura electrònica, és a dir, que no estava revocat. Per guardar l'evidència en una data determinada, la de la signatura, aquesta pot completar-se amb la informació de la validació de l'Autoritat de Certificació emissora del certificat en el moment emissió de la signatura.

   En aquest sentit, cal tenir en compte que les Autoritats de Certificació, en el moment en què un certificat digital caduca, eliminen les evidències de revocació de la seva llista de revocats, de manera que si no es guarda l'evidència esmentada en el moment de la signatura, un cop caducat el certificat, no existirà la certesa que el certificat amb què es va generar la signatura no estava revocat en el moment de generar-la.

   Per d'evitar aquest risc s'empraran signatures AdES-XL o superiors (AdES-A o PAdES-LTV) que incorporen evidències de la verificació de la validesa del certificat digital en el moment d'emetre's la signatura electrònica.

3. **Obsolescència tecnològica de la longitud de les claus criptogràfiques contingudes en el certificat digital i amb les que es generen les signatures electròniques.** Un document electrònic pot deixar de tenir validesa jurídica a partir del dia en què es posi en dubte la seguretat de les claus criptogràfiques amb les quals es va signar. En aquest escenari podrien reproduir-se de forma incontrolada signatures

generades amb les claus posades en dubte i, per tant, totes les signatures generades amb la tecnologia obsoleta es posarien en dubte.

Per resoldre aquest aspecte es requereixen claus criptogràfiques de major longitud i la generació de successius ressegellats de temps a partir de signatures electròniques que permetin aquesta possibilitat.

Per tal d'evitar aquest risc es realitzaran signatures AdES-A o PAdES-LTV i quan s'identifiqui el risc es procedirà al ressegellat de temps de totes les signatures electròniques emeses amb claus criptogràfiques la longitud de les quals resulti obsoleta.

Per tal de garantir la signatura electrònica al llarg del temps, els documents han de garantir la seva integritat mitjançant un resum criptogràfic que pugui ser comprovat abans de l'ingrés a l'arxiu electrònic conforme no han patit modificacions.

D'aquest resum criptogràfic es genera un codi únic per a cada document, que és l'evidència segura, continguda al sistema de gestió documental. Les signatures electròniques, un cop validades, s'incorporen amb aquesta evidència. Si l'evidència coincideix és correcte i es pot generar una còpia autèntica vàlida.

12. Codi Segur de Verificació (CSV)

L'article 27.3.c de la llei 39/2015 del procediment administratiu comú estableix que les còpies en suport paper de documents electrònics requereixen que hi figuri la condició de còpia i un codi generat electrònicament, o un altre sistema de verificació, que permeti contrastar l'autenticitat de la còpia mitjançant l'accés als arxius electrònics de l'òrgan o organisme públic emissor.

L'Ajuntament, per a donar resposta a aquest requeriment, utilitzen el Codi Segur de Verificació (CSV), al qual es fa referència a l'article 27.3.d de la Llei 39/2015 i que el defineix com un mecanisme a través del qual es pot comprovar la integritat d'un document imprès, acarant-lo contra el document electrònic corresponent a través de la Seu electrònica de l'Administració Pública responsable de l'emissió del document original en suport electrònic.

No obstant això, la Llei 40/2015, en l'article 42, i més recentment el Reial Decret 203/2021, en els articles 20.1 i 21, permeten la possibilitat que el Codi Segur de Verificació (CSV) es pugui emprar com a mètode de signatura en el context de l'Actuació Administrativa Automatitzada. La finalitat d'utilitzar aquest mecanisme no deixa de ser, altre cop, poder consultar i corroborar l'origen i la integritat del document a la seu electrònica de l'Administració Pública emissora.

Tanmateix, però, en l'article 21.3 del Reial Decret 203/2021 s'especifica que *en las comunicaciones de documentos electrónicos a otros órganos, organismos o entidades y cuando así lo determinen las partes implicadas*, per garantir-ne la interoperabilitat, serà necessària la vinculació d'un segell electrònic al CSV, com a mecanisme de verificació automàtica de l'origen i la integritat dels documents electrònics, segons els preceptes establerts a la NTI de Document Electrònic.

12.1 Ús del CSV

Els mecanismes d'impressió segura pels quals s'incorpora un CSV al document es preveuen amb l'objecte d'oferir un servei a les persones interessades i, per tant, té sentit incorporar-los en aquells documents que l'interessat pugui necessitar utilitzar en paper.

L'Ajuntament ha previst la distinció entre els casos d'ús de la impressió segura de documents electrònics:

1. Documents destinats exclusivament a la comunicació amb tercers.
2. Còpies de documents administratius: Els documents que no estiguin inclosos a la classificació anterior s'emetran en suport electrònic per a la seva incorporació als expedients electrònics de l'Ajuntament, sense incloure un CSV. No obstant això, els interessats podran requerir l'emissió d'una còpia en paper del document que, aleshores, incorporarà un CSV.

3. Digitalització de documents paper amb caràcter de còpia autèntica de manera que es pugui garantir la integritat del document i que el titular que aporti el document en paper en pugui verificar la seva integritat accedint a la Seu electrònica corresponent.

L'ús del CSV com a mètode de signatura acompanyat de segell d'òrgan s'ha incorporat en la present Política com a mitjà d'ús exclusiu en actuació administrativa automatitzada, per a comprovar la integritat del document mitjançant l'accés a la seu electrònica de l'Ajuntament. Es considera signatura electrònica d'acord amb el que preveu l'article 42 b) de la Llei 40/2015, de sistemes de signatura per a l'actuació administrativa automatitzada.

La utilització d'aquest sistema de signatura electrònica en les actuacions administratives automatitzades s'haurà de determinar, prèviament, mitjançant resolució de l'òrgan o càrrec competent de l'Ajuntament, d'acord amb l'article 41.2 de la Llei 40/2015 de Regim Jurídic del Sector Públic, la qual s'haurà de publicar a la seu electrònica de l'ens.

12.2 Generació del CSV

El CSV és una seqüència de lletres i números generada de manera pseudoaleatòria i associada unívocament al document.

El sistema de generació del CSV consisteix en un sistema de generació d'una URI (Uniform Resource Identifier) única per a cadascun dels documents electrònics a imprimir de forma segura o signar electrònicament.

El procés seguit per a la generació d'un document amb CSV és el següent:

- En cas de no ser un document en format PDF/A, es converteix a aquest format.
- Es genera el CSV.
- S'insereix alguna de les següents mencions, segons correspongui, en el lateral esquerre de totes les pàgines del document o en una altra ubicació alternativa que no interfereixi amb el contingut i la imatge fidel respecte al document original:

- *En aplicació de l'article 27.3.c de la Llei 39/2015, les còpies impreses d'aquest document tenen consideració de còpia autèntica, atès que el Codi Segur de Verificació (CSV): XXXXXXXXXXXXXXX permet validar la seva autenticitat, validesa i integritat a* https://mont-roig.eadministracio.cat/document-validation.1
- *Document original electrònic signat electrònicament, en aplicació de l'article 42 de la Llei 40/2015, per l'actuació administrativa automatitzada XXX - nom actuació - XXXX regulada per XXXX - normativa AAA -XXXXX atès que el Codi Segur de verificació (CSV): XXXXXXXXXXXXXXX permet validar la seva autenticitat, validesa i integritat a* https://mont-roig.eadministracio.cat/document-validation.1

12.3 Procediment de validació de documents amb CSV

Per a l'acarament dels documents que inclouen CSV, els interessats s'han d'adreçar a la Seu electrònica. A través de la Seu es podrà accedir al Validador de documents electrònics amb CSV i comprovar, d'aquesta manera, l'autenticitat del document, tal i com es descriu al capítol 7 del MGDE.

12.4 Procediment de signatura amb CSV en Actuació Administrativa Automatitzada

L'article 42.b de la llei 40/2015 de Règim Jurídic de el Sector Públic regula l'ús del Codi Segur de Verificació (CSV) com a mitjà de signatura, vinculat a l'Administració Pública, òrgan, organisme públic o entitat de dret públic, permet en tot cas la comprovació de la integritat del document mitjançant l'accés a la seu electrònica corresponent.

Aquest sistema, que només es pot utilitzar en actuació administrativa automatitzada, consisteix a afegir un codi únic de verificació a un document perquè es pugui validar la seva autenticitat a través de l'accés a la seu electrònica.

Tal com s'ha esmentat anteriorment, es podrà utilitzar aquest sistema de signatura electrònica en les actuacions administratives automatitzades que es determini prèviament mitjançant resolució de l'òrgan o càrrec competent de l'Ajuntament, d'acord amb l'article 41.2 de la Llei 40/2015 de Regim Jurídic del Sector Públic, que es publicarà a la seu electrònica.

13. Admissió de mecanismes d'identificació electrònica

L'admissió del mecanismes d'identificació i signatura electrònica es realitza d'acord amb els nivells de seguretat estipulats a l'Annex del Reglament d'Execució 2015/1502 de la Comissió Europea i a l'Esquema Nacional de Seguretat, en relació amb la Llei Orgànica de Protecció de Dades de Caràcter Personal.

Els mecanismes d'identificació i signatura electrònica considerats admissibles per als tràmits d'una categoria determinada ho són també pels tràmits classificats de categoria inferior a aquesta. Així doncs, quan en el context d'un servei electrònic sigui necessari garantir la protecció de la confidencialitat de les dades implicades mitjançant mecanismes d'identificació electrònica, s'admetran els següents mecanismes:

13.1.1 Per a tràmits de categoria Alta

Per aquesta mena de tràmits s'accepten els sistemes d'identificació electrònica de nivell de seguretat alt, com aquells que fan un registre dels usuaris, presencial i fiable, i proveeixen els usuaris d'un mitjà d'identificació electrònica de doble factor. S'admeten amb caràcter obligatori:

- Aquells certificats reconeguts o qualificats que s'emetin en un dispositiu qualificat de creació de signatura electrònica, entre els establerts en el punt 9.5. d'aquesta Política, atenent a les tipologies de certificats i del col·lectiu concret.
- Qualsevol dels mitjans d'identificació que hagi estat notificat de nivell de seguretat alt i s'inclogui a la llista que, conforme al que estableix el ReIDAS en el capítol 2, publicarà la Comissió Europea per accedir als serveis prestats en línia per un organisme del sector públic en un Estat Membre, a efectes de l'autenticació transfronterera.

13.1.2 Per a tràmits de categoria Mitjana

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

- Obligatòriament, els certificats reconeguts o qualificats i els certificats reconeguts o qualificats de segell electrònic establerts en el punt 9.5 d'aquesta Política, atenent a les tipologies de certificats i del col·lectiu específic.

- Obligatòriament, qualsevol dels mitjans d'identificació que hagi estat notificat de nivell de seguretat substancial i s'inclogui a la llista que, conforme al que estableix el ReIDAS al capítol 2, publicarà la Comissió Europea per accedir als serveis prestats en línia per un organisme del sector públic en un Estat Membre, a efectes de l'autenticació transfronterera.
- Els mecanismes IdCAT Mòbil i Cl@ve (Cl@ve PIN, Cl@ve Permanente i Cl@ve Firma).
- Qualsevol altre mecanisme integrat al servei VALid operat pel Consorci AOC i classificat nivell mig d'acord amb les especificacions marcades per l'Esquema Nacional de Seguretat i del Reglament d'Execució 2015/1502 de la Comissió Europea.

13.1.3 Per a tràmits de categoria Baixa

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

14. Admissió de mecanismes de signatura electrònica

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

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

Els mecanismes de signatura electrònica considerats admissibles per als tràmits classificats d'una categoria determinada són també admissibles per a les actuacions classificades de categoria inferior a aquesta. En particular, quan en el context d'un servei electrònic es requereixi una signatura electrònica s'admetran les següents signatures:

14.1.1 Per a tràmits de categoria Alta

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

- *Respecte dels formats:* Els serveis electrònics oferts pels organismes dels Estats Membres de la Unió Europea han de reconèixer les signatures qualificades que siguin conformes a algun dels formats de referència que es definiran per a les signatures qualificades, o que s'hagin generat amb els mètodes de referència, quan siguin d'un format alternatiu, segons el que estableix a l'article 27 del ReIDAS, a efectes de garantir la interoperabilitat en l'accés transfronterer a serveis públics.
- *Respecte dels certificats emprats:* S'han d'admetre les signatures electròniques generades amb aquells certificats reconeguts o qualificats de signatura electrònica, entre els considerats a l'apartat 15.2 de la present Política, que s'emetin en un dispositiu qualificat de creació de signatura electrònica. També els segells electrònics generats amb aquells certificats de segell electrònic, reconeguts o qualificats, entre els que s'especifiquen a l'apartat 15.2, que s'emetin en un dispositiu qualificat de creació de segells electrònics i atenent a les tipologies de certificats que es llisten per a cadascun dels col·lectius que allà es distingeixen.

14.1.2 Per a tràmits de categoria Mitjana

Seran admissibles les signatures electròniques avançades i els segells electrònics avançats que es fonamentin en un procediment de registre fiable de la identitat dels usuaris. També les

signatures electròniques avançades basades en un certificat reconegut o qualificat de signatura electrònica i els segells electrònics avançats basats en certificats qualificats de segell electrònic, conforme al que s'estableix als articles 27.1 i 37.1 del ReIDAS, així com les signatures electròniques ordinàries generades a partir d'un mecanisme d'identificació de nivell de seguretat substancial, com els considerats a l'apartat 9.5.1. d'aquesta Política. En concret:

- *Respecte del format:* s'hauran de reconèixer les signatures electròniques avançades i les signatures avançades basades en un certificat qualificat de signatura electrònica que siguin conformes a algun dels formats de referència definits al Reglament d'Execució 2015/1506 de la Comissió Europea, o que s'hagin generat amb els mètodes de referència, quan siguin d'un format alternatiu, segons el que estableix a l'article 27 del ReIDAS, a efectes de garantir el correcte tractament dels documents signats electrònicament en l'ús transfronterer de serveis públics.
- *Respecte dels certificats emprats:* s'hauran d'admetre les signatures electròniques generades amb els certificats de signatura electrònica considerats a l'apartat 10.2 de la present Política. També els segells electrònics generats amb els certificats de segell electrònic considerats en el mateix apartat 10.2, atenent a les tipologies de certificats que es llisten per a cadascun dels col·lectius que allà es distingeixen.
- Seran admissibles les signatures ordinàries basades en els mecanismes IdCAT Mòbil i Cl@ve (Cl@ve PIN, Cl@ve Permanente i Cl@ve Firma).
- També les signatures ordinàries basades en qualsevol altre mecanisme que hagi estat classificat de nivell mig o substancial i integrat com a tal al servei VÀLid del Consorci AOC.

14.1.3 Per a tràmits de categoria Baixa

S'admeten els mecanismes que generen signatures electròniques ordinàries prenent com a fonament un mecanisme d'identificació de nivell de seguretat baix, com els descrits a l'apartat 13.1.3.

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

A continuació es reuneixen els criteris essencials vinculats a la implantació de mecanismes d'identificació i signatura electrònics en relació amb els nivells de seguretat descrits amb anterioritat.

15.1 Criteri general

S'estableix com criteri general que per a la identificació i signatura electrònica en els tràmits o serveis electrònics s'admetran els mecanismes d'identificació i signatura classificats amb nivell de seguretat mitjà o substancial, conforme als apartats 13.1.2 i 13.2.2.

15.2 Criteris d'aplicació de nivell alt de seguretat

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

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

15.3 Criteris d'aplicació de nivell baix de seguretat

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

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

16. Normatives de signatura electrònica

Una normativa de signatura electrònica és un document que conté un conjunt de normes relatives a la signatura electrònica, en un context particular (contractual, jurídic, legal, ...), que té per objectiu poder determinar la validesa d'una signatura electrònica en una transacció en concreta.

Aquestes normatives s'organitzen sobre els conceptes de generació i validació de la signatura electrònica i defineixen les regles i obligacions de tots els actors involucrats en aquests processos. En aquest sentit, especifiquen la informació que ha d'incloure el signant en el procés de generació de la signatura i la informació que ha de comprovar i complementar el verificador en el procés de validació de la mateixa.

L'Ajuntament de Mont-roig del Camp i les entitats que en depenen fan servir les normatives de signatura electrònica compartides sota llicència d'ús BY - NC - SA de Creative Commons per l'empresa Astrea la Infopista Jurídica SL i que es pot consultar de forma actualitzada al següent enllaç: http://astrea.es/web12/spcesp.htm.

Una vegada dintre d'aquest enllaç, per a accedir a les normatives de signatura electrònica, haurà de consultar-se l'Annex II sobre Estàndards tècnics de la Política de Seguretat Documental proposada per Astrea.

Astrea, amb la publicació de la biblioteca del estàndards tècnics de signatura electrònica, pretén facilitar a les eines de creació i de validació de signatures electròniques l'automatització dels processos de tractament de les mateixes, d'acord amb l'estàndard tècnic de signatura electrònica seleccionada en cada cas, mitjançant l'establiment d'unes regles bàsiques, que siguin comuns per a totes les administracions públiques. D'aquesta manera s'homogeneïtza el contingut tècnic de les signatures electròniques i s'afavoreix la interoperabilitat de les signatures electròniques en les relacions interadministratives, d'acord amb el que estableix l'Esquema Nacional d'Interoperabilitat.

En aquest sentit, les diferents normatives de signatura electrònica incorporen compromisos de signatura, que són particularitzacions de la política general, i que permeten definir amb major granularitat els controls sobre les regles de creació i validació de les signatures electròniques com poden ser: els nivells de seguretat acceptats en el certificat de firma, rol o càrrec del responsable de produir la signatura, etc.

A la biblioteca d'Astrea es recullen els estàndards de signatura electrònica associada als actes administratius més rellevants dins dels procediments telemàtics de les administracions públiques. En total es recullen fins a 34 normatives de signatura electrònica, les quals es relacionen a continuació:

- **Acte de ciutadà (5.1.1.1 ETSEAJ)**
    - Acte de declaració de voluntat (5.1.1.2 ETSEAJ)

        - Acte de sol·licitud de ciutadà (5.1.1.3 ETSEAJ)
        - Acte de conformitat de ciutadà (5.1.1.4 ETSEAJ)
        - Acte negocial de ciutadà (5.1.1.34 ETSEAJ)
    - Acte de comunicació prèvia de ciutadà (5.1.1.5 ETSEAJ)
    - Acte de declaració responsable de ciutadà (5.1.1.6 ETSEAJ)
    - Acte de queixa o suggeriment de ciutadà (5.1.1.33 ETSEAJ)
- **Acte de l'Administració (5.1.1.7 ETSEAJ)**
    - Acte administratiu (5.1.1.8 ETSEAJ)
        - Acte resolutori o de tràmit definitiu (5.1.1.9 ETSEAJ)
        - Acte de simple tràmit (5.1.1.10 ETSEAJ)
        - Acte de comunicació electrònica (5.1.1.11 ETSEAJ)
            - Acte de recepció electrònica (5.1.1.12 ETSEAJ)
            - Acte de notificació electrònica (5.1.1.13 ETSEAJ)
            - Acte de transmissió electrònica de datos (5.1.1.14 ETSEAJ)
        - Acte de constància (5.1.1.15 ETSEAJ)
            - Acte de publicació (5.1.1.16 ETSEAJ)
            - Acte de còpia autèntica (5.1.1.17 ETSEAJ)
                - Acte de còpia autèntica compulsada (5.1.1.18 ETSEAJ)
                - Acte de còpia autèntica migrada (5.1.1.19 ETSEAJ)
                - Acte de còpia autèntica digitalitzada (5.1.1.20 ETSEAJ)
            - Acte de còpia simple (5.1.1.21 ETSEAJ)
            - Acte d'aixecament d'acta (5.1.1.22 ETSEAJ)
            - Acte certificant (5.1.1.23 ETSEAJ)
        - Acte consultiu (5.1.1.24 ETSEAJ)
        - Acte vistiplau de l'Administració (5.1.1.25 ETSEAJ)
        - Acte de foliat (5.1.1.26 ETSEAJ)
        - Acte de fiscalització (5.1.1.27 ETSEAJ)
        - Acte de proposta (5.1.1.28 ETSEAJ)

- Acte de donació de fe (5.1.1.29 ETSEAJ)
- Acte de sol·licitud de l'Administració (5.1.1.31 ETSEAJ)
- Acte de declaració responsable de l'Administració (5.1.1.32 ETSEAJ)

- Acte negocial (5.1.1.30 ETSEAJ)

17. Casos d'ús de la signatura electrònica

Prèviament a la descripció dels casos d'ús identificats de signatura electrònica, és necessari definir els conceptes claus en aquest entorn: l'expedient administratiu completament electrònic i el seu foliat del qual en resulta un document d'índex també electrònic. Per aquest motiu, es parteix de la definició que fa la Llei 39/2015 al seu article 70:

- S'entén per expedient administratiu el conjunt ordenat de documents i actuacions que serveixen d'antecedent i fonament a la resolució administrativa, així com les diligències encaminades a executar-la.
- Els expedients tindran format electrònic i es formaran mitjançant l'agregació ordenada de quants documents, proves, dictàmens, informes, acords, notificacions i altres diligències hagin d'integrar-los, així com un índex numerat de tots els documents que contingui quan es remeti. Així mateix, ha de constar a l'expedient la còpia electrònica certificada de la resolució adoptada.
- Quan en virtut d'una norma calgui remetre l'expedient electrònic, es farà d'acord amb el que preveu l'Esquema Nacional d'Interoperabilitat i en les corresponents Normes Tècniques d'Interoperabilitat i s'enviarà complet, foliat, autentificat i acompanyat d'un índex, també autenticat, dels documents que contingui. L'autenticació de l'esmentat índex garantirà la integritat i immutabilitat de l'expedient electrònic generat des del moment de la seva signatura i permetrà la recuperació sempre que calgui, i és admissible que un mateix document formi part de diferents expedients electrònics.

D'acord amb aquests preceptes, l'índex de l'expedient es guardarà en un fitxer XML, que haurà d'estar signat amb un segell electrònic de l'Ajuntament. Aquesta signatura serà en format XML i, més concretament, en XAdES-A.

Després de la definició dels conceptes d'expedient electrònic i de foliat del mateix, es descriuen els diferents escenaris de signatura electrònica identificats:

17.1 Signatura electrònica d'un document electrònic

Permet signar electrònicament documents en suport electrònic en qualsevol moment del seu cicle de vida, ja siguin documents creats o generats electrònicament per altres aplicacions.

Les principals característiques d'aquest escenari són:

- Es realitza la signatura sobre un document original o una còpia d'un original, en suport electrònic.
- El document original o la còpia i les signatures s'han d'incorporar al sistema.

- Per tal d'assegurar la integritat i l'autenticitat de la signatura rebuda de l'aplicació de creació de signatures, serà necessari validar-la i completar-la utilitzant un servei o a través d'una Autoritat de Validació.
- Cal incorporar al sistema l'evidència de validació, que serà la signatura completada, la qual serà en el cas de XML el mateix document amb signatura attached i per PDF el mateix document amb signatura attached o dettached.
- El document electrònic estarà en qualsevol format dels acceptats per l'Ajuntament segons el Catàleg de formats de documents electrònics publicat a la Seu electrònica, preferiblement PDF/A i XML, sempre que sigui necessari garantir la seva preservació al llarg del temps.
- El document es podrà signar diverses vegades i per diferents usuaris.
- Es podrà signar amb el sistema de signatura electrònica basada en certificat electrònic del signant o bé amb signatura a través d'acreditació de la identitat i d'evidències de la voluntat de signatura.
- Es podrà signar en paral·lel i/o de forma niuada.
- En el cas de documents que no s'hagin de guardar més enllà de la validesa del segell de temps, la signatura (en el cas de la signatura a través d'acreditació de la identitat i evidències de voluntat o biomètrica, la signatura es refereix a la signatura secundària) es generarà en format AdES-T o, si no és possible, es completarà a aquest format.
- En el cas de documents que s'hagin de guardar més enllà de la validesa del segell de temps, la signatura electrònica es generarà o es completarà a AdES-A. Per als documents PDF serà PAdES-LTV o XAdES-A en cas de signatures dettached, i per als documents XML serà XAdES-A.

Finalment, concretant el tipus de signatura, s'estableixen les següents característiques o requeriments:

- **Classe de signatura:** Avançada o Reconeguda.
- **Sistema de signatura:**
    - Amb certificat electrònic. Per a les signatures generades per l'Ajuntament serà el certificat de treballador o el certificat de segell electrònic. Els ciutadans i les empreses podran utilitzar qualsevol dels certificats definits en el punt 10.2 del present document.
    - Amb signatura a través d'acreditació de la identitat i d'evidències de la voluntat de signatura. Podran generar aquest tipus de signatura els treballadors de l'Ajuntament en tràmits concrets i els ciutadans. Les empreses no podran utilitzar aquest tipus de signatura a no ser que s'acrediti mitjançant el gestor de

representacions que utilitzi l'Ajuntament la capacitat de representació de la persona que signa.

- **Formats:** PAdES. Inicialment en format PAdES-T. En el cas de preservació es completarà la signatura a format PAdES-LTV.
- **Segell de temps:** Sí.
- **Nivell de signatura:** Simple, Múltiple (niuada o en paral·lel).
- **Tipus de signatura**: Attached o Dettached.
- **Normativa de signatura:**
    - En el cas de signatura emesa pel ciutadà: Acte de ciutadà (5.1.1.1 ETSEAJ)
    - En el cas de signatura emesa per l'Ajuntament, ens que en depèn o qualsevol altra Administració Pública: Acte de l'Administració (5.1.1.7 ETSEAJ).

17.2 Digitalització certificada de documents en paper: còpia certificada electrònica

Les principals característiques d'aquest escenari són:

- Consisteix en la signatura electrònica d'un document digitalitzat, en format PDF, per crear una còpia simple electrònica amb evidències.
- La signatura és necessària per a garantir la integritat i evidències d'autenticitat del procés de digitalització, així com la data de la digitalització.
- El personal de l'Ajuntament de Mont-roig del Camp que digitalitza la documentació és el responsable de comprovar la fidelitat de la còpia electrònica amb el document digitalitzat i utilitza la seva signatura per avalar aquest fet, sobre el document digitalitzat. El personal ha d'estar habilitat per fer-ho.
- Els documents digitalitzats es signen incorporant un segell de temps. Es genera una signatura PAdES-T.
- Per tal d'assegurar la integritat i les evidències d'autenticitat de la signatura rebuda de l'aplicació de creació de signatures serà necessari validar-la.
- En el cas que els documents s'hagin de guardar més enllà de la validesa del segell de temps, la signatura electrònica es generarà o es completarà a PAdES-LTV.

Finalment, concretant el tipus de signatura, s'estableixen les següents característiques o requeriments:

- **Classe de signatura:** Avançada
- **Tipus de certificat:** Certificat de treballador o Certificat de Segell Electrònic.
- **Formats:** PAdES. Inicialment en format PAdES-T. En el cas de requerir-se preservació més enllà del segell de temps es completarà la signatura a format PAdES-LTV.
- **Segell de temps:** Sí.
- **Nivell de signatura:** Simple.
- **Tipus de signatura:** Attached.
- **Normativa de signatura:** Acte de còpia autèntica digitalitzada (5.1.1.20 ETSEAJ).

17.3 Còpia electrònica «certificada» d'un document electrònic signat electrònicament

Permet obtenir còpies electròniques autèntiques de documents originals signats electrònicament aplicant un canvi de format. Aquest seria, per exemple, el cas de la migració de formats en casos d'obsolescència tecnològica.

Les principals característiques d'aquest escenari són:

- A partir d'un document signat electrònicament s'obté una còpia (per exemple, PDF/A o un altre format de preservació) certificada digitalment per guardar-la a l'arxiu electrònic.
- La còpia del document electrònic ha d'estar en un format normalitzat i estandarditzat abans de signar-la.
- El document se signarà automàticament una única vegada amb segell electrònic titularitat de l'Ajuntament de Mont-roig del Camp i previst exclusivament per a aquesta finalitat.

Finalment, concretant el tipus de signatura s'estableixen les següents característiques o requeriments:

- **Classe de signatura:** Avançada.
- **Tipus de certificat:** Certificat de Segell Electrònic.
- **Formats:** Dependrà del format final. Si és PDF/A es generarà en format PAdES-LTV.
- **Segell de temps:** Sí.
- **Nivell de signatura:** Simple.

- **Tipus de signatura:** Attached o dettached.
- **Normativa de signatura:** Acte de còpia autèntica compulsada (5.1.1.18 ETSEAJ).

17.4 Processos de signatura automatitzada

Permet la signatura de diversos documents de forma automàtica amb un nivell important de garanties jurídiques. No requereix la intervenció del signant en el procés de signatura, atès que només pot ser realitzada amb certificats de segell electrònic.

Les principals característiques d'aquest escenari són:

- Signatura de diversos documents de forma automàtica.
- El document electrònic pot estar en qualsevol format dels acceptats (PDF i XML).
- Es guardaran al repositori segur del servidor de l'Ajuntament tant els certificats digitals com les corresponents claus públiques que han de permetre generar processos de signatura automatitzada.

Un cop descrites les característiques concretes d'aquest escenari, s'enumeren els criteris d'aplicació i actuació:

- Aquest escenari està pensat per aquelles tasques en què s'han de signar diversos documents de forma automatitzada amb garanties jurídiques.
- S'utilitzarà el CSV com a mètode de signatura i un certificat de segell electrònic corresponent a un òrgan administratiu que signarà els documents en nom de l'aplicació i de l'Ajuntament de Mont-roig del Camp.
- Hi haurà una evidència genèrica via normativa d'actuació administrativa automatitzada de que el responsable del certificat emmagatzemat al repositori segur de l'Ajuntament ha autoritzat la signatura automatitzada.

Concretant el tipus de signatura s'estableixen les següents característiques o requeriments:

- **Classe de signatura:** Avançada .
- **Tipus de certificat:** Certificat de Segell Electrònic.
- **Formats:** Per a documents XML serà XAdES-T i per a la seva conservació XAdES-A. Per a documents PDF serà PAdES-T i per a la seva conservació PAdES-LTV.
- **Segell de temps:** Sí.
- **Nivell de signatura:** Simple.
- **Tipus de signatura:** Attached.

- **Normativa de signatura:** Acte de l'Administració (5.1.1.7 ETSEAJ), aquella que sigui d'aplicación segons el tipus de document generat o acte realitzat.

Aquest és un escenari que abasta diversos àmbits que es podrien arribar a identificar com a sub-escenaris diferents com, per exemple:

- Signatura automatitzada en processos de digitalització ordinària massiva.
- Procediments d'intercanvi d'informació amb altres administracions.
- Emissió de documents de constància en registres administratius.

17.5 Signatura electrònica biomètrica d'un document electrònic

Permet signar electrònicament documents en suport electrònic en qualsevol moment del seu cicle de vida, ja siguin documents creats o generats electrònicament per altres aplicacions.

Les principals característiques d'aquest escenari són:

- Es realitza la signatura sobre un document original en suport electrònic.
- La signatura forma part del mateix document.
- Els documents originals amb les seves signatures s'han d'incorporar al sistema.
- El mateix sistema garanteix la integritat i l'autenticitat de la signatura de manera que no serà necessari validar-la.
- En cas que el document s'hagi de guardar al llarg del temps es procedirà a la seva signatura electrònica avançada amb un segell electrònic. En aquest cas, sí que s'haurà de validar la signatura avançada corresponent incorporant al sistema l'evidència de validació que serà la signatura completada que, atenent que es tractarà de documents de format PDF, estarà en el mateix document amb signatura attached.
- El document electrònic estarà en format PDF o PDF/A.
- El document es podrà signar diverses vegades i per diferents usuaris.
- Es podrà signar només en paral·lel.
- En cas que els documents s'hagin de guardar durant llargs períodes de temps, la signatura electrònica que es generarà amb el segell electrònic serà en format PADES-LTV.

Finalment, concretant el tipus de signatura, s'estableixen les següents característiques o requeriments:

- **Classe de signatura:** Avançada.

- **Tipus de certificat:** Pel xifrat de les dades biomètriques i el resum criptogràfic del document, la clau pública del certificat de xifrat estarà guardada en els servidors de l'Ajuntament i la privada en un tercer de confiança. Per a les signatures generades amb el segell electrònic de l'Ajuntament, serà el Certificat de Segell Electrònic.
- **Formats:**
    - **Signatura biomètrica:** Signatura específica.
    - **Signatura amb segell electrònic:** PAdES en format PAdES-LTV.
- **Segell de temps:** Sí (per a la signatura del segell electrònic).
- **Nivell de signatura:** Simple o Múltiple (niuada o en paral·lel).
- **Tipus de signatura:** Attached.
- **Normativa de signatura:** aquella que sigui d'aplicació segons el tipus de document generat o acte realitzat.

17.6 Incorporació de documents signats digitalment per part del tercer

En el cas que un tercer lliuri un document signat electrònicament amb sistemes de signatura que estiguin sota el seu control caldrà:

- Validar les signatures electròniques del document.
- Si les signatures no són AdES-T o AdES-A / LTV es procedirà a completar-les fins a un d'aquests nivells en funció del temps que s'hagi de guardar el document.
- A continuació, es procedirà a incorporar al sistema el document amb les seves signatures completades.

Finalment, concretant el tipus de signatura, s'estableixen les següents característiques o requeriments:

- **Classe de signatura:** Avançada o Reconeguda en funció dels certificats utilitzats per a la seva signatura.
- **Tipus de certificat:** Qualsevol certificat definit en el punt 10.2 del present document.
- **Formats:** Per documents XML serà XAdES-T i per a la seva conservació XAdES-A. Per a documents PDF serà PAdES-T i per a la seva conservació PAdES-LTV.
- **Segell de temps:** S'aconsella aplicar-ne, tot i que dependrà del tercer. Un cop completada la signatura, sí.
- **Nivell de signatura:** Simple o Múltiple (niuada o en paral·lel).

- **Tipus de signatura:** Attached.
- **Normativa de signatura:** Acte de ciutadà (5.1.1.1 ETSEAJ)

Annex I - Conceptes

Per poder copsar i comprendre millor el que exposa i regula la present Política s'ha considerat adient incorporar un capítol de definició de termes relacionats amb la signatura electrònica i els certificats digitals.

- **Casos d'ús de la signatura electrònica:** Entès com els possibles escenaris de generació de documents electrònics signats. Per a cada cas d'ús s'identifiquen els possibles sistemes de signatura, formats de signatura electrònica, nivells de signatura, la normativa de signatura electrònica a aplicar, etc.

  Es defineixen sis tipus de casos d'ús diferents:

  - Signatura electrònica d'un document electrònic
  - Digitalització certificada de documents en paper
  - Còpia electrònica certificada d'un document electrònic signat electrònicament
  - Processos de signatura automatitzada
  - Signatura electrònica biomètrica d'un document electrònic
  - Incorporació de documents signats electrònicament per part d'un tercer
- **Classes de signatura electrònica:** Classes i validesa jurídica de la signatura electrònica segons es defineix en el Reglament Europeu (UE) 910/2014 relatiu a la identificació electrònica i els serveis de confiança en les transaccions electròniques en el mercat interior: signatura simple o ordinària, avançada i reconeguda.
- **Codi segur de verificació (CSV):** Codi que s'inclou en els documents electrònics que puguin ser impresos i que, a partir de la confrontació d'aquest codi a la seu electrònica de l'Ajuntament, un tercer pugui verificar l'originalitat d'aquesta impressió del document electrònic. Tanmateix, també pot esdevenir un mecanisme de signatura, acompanyat de segell d'òrgan, en el decurs de l'Actuació Administrativa Automatitzada, o bé un mètode de signatura electrònica per part del personal de l'Ajuntament.
- **Document electrònic:** Informació de qualsevol naturalesa, en forma electrònica, arxivada en un suport electrònic segons un format determinat i susceptible d'identificació i tractament diferenciat.
- **Estàndard:** Especificació tècnica aprovada per un organisme de normalització reconegut per a una aplicació repetida o continuada, el compliment de la qual no sigui obligatòria i que estigui inclosa en una de les següents categories:

  - Norma internacional: norma adoptada per una organització internacional de normalització i posada a disposició del públic.
  - Norma europea: norma adoptada per un organisme europeu de normalització i posada a disposició del públic.
  - Norma nacional: norma adoptada per un organisme nacional de normalització i posada a disposició del públic.

- **Expedient electrònic:** Conjunt de documents electrònics corresponents a un procediment administratiu, sigui quin sigui el tipus d'informació que continguin. A l'efectuar-ne el tancament formal, se n'ha de generar la foliació i l'índex autenticat.
- **Signatura electrònica:** Conjunt de dades en forma electrònica, consignades juntament amb altres o associades amb elles, que poden ser utilitzades com a mitjà d'identificació del signant.
- **Signatura electrònica avançada:** Signatura electrònica que permet identificar el signant i detectar qualsevol canvi ulterior de les dades signades, que està vinculada al signant de manera única i a les dades a què es refereix i que ha estat creada per mitjans que el signant pot mantenir sota el seu exclusiu control. Pot estar basada en un certificat reconegut o amb evidències d'autenticació.
- **Signatura electrònica reconeguda:** Signatura electrònica avançada basada en un certificat reconegut i generada mitjançant un dispositiu segur de creació de signatura.
- **Signatura biomètrica:** Tecnologia que permet capturar dades biomètriques durant el procés de signatura manuscrita sobre dispositius electrònics. Principalment, les dades biomètriques capturades durant el procés de signatura són la pressió del llapis, la velocitat d'escriptura i l'acceleració.
- **Format de signatura electrònica:** Forma en què es codifiquen les signatures electròniques. Els formats més utilitzats són els formats S/MIME, CMS, XAdES, CAdES i PAdES.
- **Llista de serveis de confiança (TSL):** Llista, d'accés públic, que recull informació precisa i actualitzada d'aquells serveis de certificació i signatura electrònica que es consideren aptes per al seu ús en un marc d'interoperabilitat de les administracions públiques espanyoles i europees.
- **Nivell de signatura:** Indica si el document té una única signatura o múltiples signatures, i en aquest darrer cas si es generen en paral·lel o niuades.
- **Normativa de signatura electrònica:** Documents que detallen les normes relatives a la signatura electrònica, organitzades al voltant dels conceptes de generació i validació de signatura i en un context particular com, per exemple, contractual i que defineix les

regles i les obligacions de tots els actors involucrats en aquest procés. L'objectiu d'aquest procés és determinar la validesa de la signatura electrònica per als diferents tipus de transacció.

- **Segellat de temps:** Acreditació, a càrrec d'un tercer de confiança, de la data i hora de realització de qualsevol operació o transacció per mitjans electrònics.
- **Sistema de signatura:** Forma en què se signa un document electrònic, ja sigui mitjançant un certificat digital reconegut del signant, amb un sistema d'identificació més evidència electrònica de l'acte de la signatura o mitjançant signatura biomètrica.
- **Tipus de signatura:** Forma com es relaciona la signatura electrònica amb el document signat: dins del mateix document, com un document a part o dins d'estructures XML.

Annex II - Normativa aplicable i estàndards internacionals

La recent revolució en l'ús del document electrònic és el resultat de l'aparició de canvis normatius que han donat impuls a les eines telemàtiques i han equiparat, en determinades circumstàncies, els documents en format electrònic als documents en formats més tradicionals.

A més, tant a nivell nacional com de la Unió Europea o internacionalment, les organitzacions d'estandarditzación tècnica han definit i documentat els criteris i formats a utilitzar per a la gestió dels documents digitals en tots els seus aspectes, garantint la seva validesa jurídica.

En aquest apartat s'identifiquen el conjunt de normatives i estàndards internacionals que s'han tingut en compte per a la definició de la Política d'Identificació i Signatura Electrònica de l'Ajuntament de Mont-roig del Camp.

Normativa aplicable

a. Àmbit europeu:

- Reglament Europeu (UE) 910/2014 del Parlament Europeu i Consell, relatiu a la identificació electrònica i els serveis de confiança en les transaccions electròniques en el mercat interior. Conegut com Reglament eIDAS.
- 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 de l'anterior Reglament.

b. Àmbit estatal:

- Llei 15/2014, de 16 de setembre, de racionalització del sector públic i altres mesures de reforma administrativa.
- Llei 25/2015, de 28 de juliol, de mecanisme de segona oportunitat, reducció de la càrrega financera i altres mesures d'ordre social.
- Llei 39/2015 d'1 d'octubre de procediment administratiu comú de les administracions públiques
- Llei 40/2015 d'1 d'octubre, de règim jurídic del Sector Públic

- Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.
- Reial Decret 3/2010 de 8 de gener de l'Esquema Nacional de Seguretat.
- Reial Decret 4/2010 de 8 de gener de l'Esquema Nacional d'Interoperabilitat.
- 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 4 de febrer de 2011, de la Presidència de l'Agència Estatal d'Administració Tributària, sobre l'ús del codi segur de verificació i per la qual es creen segells electrònics de l'organisme.
- Resolució de 19 de juliol de 2011 de la Norma Tècnica d'Interoperabilitat d'Expedient Electrònic.
- Resolució de 19 de juliol de 2011, de la Norma tècnica d'interoperabilitat de Document Electrònic.
- Resolució de 27 d'octubre de 2016, de la Norma tècnica d'interoperabilitat de política de signatura i segell electrònic i de certificats de l'Administració.
- Resolució de 14 de juliol de 2017, de la Secretaria General de l'Administració Digital, segons la qual s'estableixen les condicions d'ús de la 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.

c. Àmbit autonòmic

- Llei 26/2010, de 3 d'agost, de règim jurídic i procediment a les administracions públiques de Catalunya.
- Llei 29/2010, de 3 d'agost, de mitjans electrònics en el sector públic.
- Decret 76/2020, de 4 d'agost, d'Administració digital.
- ACORD GOV/92/2015, de 16 de juny, pel qual s'aprova el sistema d'identificació electrònica idCAT-SMS i l'ús del Validador de credencials d'identitat.

Estàndards internacionals i altres convencions

- Estàndards tècnics de signatura electrònica compartits sota la llicència d'ús BY - NC - SA de Creative Commons de l'empresa Astrea la Infopista Jurídica SL: http://astrea.es/web12/biblioesp/_estandares-tecnicos/

- ETSE RFC 2315 (1998), ETSE RFC 2630 (1999), IETF RFC 3369 (2002), IETF RFC 3852 (2004): PKCS # 7: Cryptographic Message Syntax (CMS)
- ETSI TS 101 733. v.1.6.3, v1.7.4 i v.1.8.1: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)
- ETSI TS 119 122-3: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures: Part 3: incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES.
- ETSE TR 119 124-1: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.
- ETSI TS 119 124-2: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of CAdES baseline signatures.
- ETSI TS 119 124-3: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended CAdES signatures.
- ETSI TS 119 124-4: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of CAdES baseline signatures.
- ETSI TS 119 124-5: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of extended CAdES signatures.
- ETSE TR 119 134-1 Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.
- ETSI TS 119 134-2: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of XAdES baseline signatures.
- ETSI TS 119 134-3: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended XAdES signatures.
- ETSI TS 119 134-4: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of XAdES baseline signatures.

- ETSI TS 119 134-5: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of extended XAdES signatures.
- ETSI TS 119 142-3: Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS).
- ETSE TR 119 144-1 Electronic Signatures and Infrastructures (ESI); PAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.
- ETSI SR 019 020: The framework for Standardization of signatures; Standards for AdES digital signatures in mobile and distributed environments.
- IETF RFC 5280 (2008): Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- IETF RFC 2560 (1999): X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol - OCSP
- IETF RFC 3126 (2001): Electronic Signature Formats for Long Term Electronic Signatures.
- ISO 19005 (2008): Format del fitxer / A-1
- ISO / TR 18492: 2005- Long-term preservation of electronic document-based Information
- UNE-ISO / TR 13008: 2010- Informació i documentació. Conversió de documents digitals i processos de migració.
- ETSI TS 102 176-1 V2.0.0 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
- ETSI TS 102 023, v.1.2.1 i v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- Policy requirements for time-stamping authorities.
- ETSI TS 101.861 V1.3.1 Time stamping profile.
- ETSE TR 102.038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.
- ETSE TR 102.041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.
- ETSE TR 102.045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.

- ETSE TR 102.272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.
- IETF RFC 2560, X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP.
- IETF RFC 3125, Electronic Signature Policies.
- IETF RFC 3161 actualitzada per RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- IETF RFC 5280, RFC 4325 i RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.
- IETF RFC 5652, RFC 4853 i RFC 3852, Cryptographic Message Syntax (CMS).
- ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".